Información legal

Tabla de contenido

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 la versión más reciente de esta guía y otros recursos de documentación de DRA, visite el sitio Web de documentación de DRA (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Información de contacto

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y el resto de la documentación incluida con este producto. Puede utilizar el enlace de **comentarios de este tema** en la parte inferior de cada página de la documentación en línea o bien enviar un mensaje de correo electrónico a Documentation-Feedback@microfocus.com.

Para obtener información sobre problemas de productos específicos, póngase en contacto con el servicio de atención al cliente de Micro Focus en https://www.microfocus.com/support-and-services/.

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 ¿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 Microsoft Active Directory, Windows, Exchange y Azure Active Directory.

- **Compatibilidad con Azure y Active Directory local, Exchange y Skype Empresarial:** Ofrece una gestión administrativa de Azure y Active Directory local, Active Directory, Exchange Server local, Skype Empresarial local, 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.

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 (La persona encargada del mantenimiento de la configuración del producto)	Consola de delegación y configuración	Servidor principal
Administrador avanzado	Configuración de DRA Reporting Center (NRC) PowerShell *(opcional)* CLI *(opcional)* Proveedor ADSI de DRA *(opcional)*	Cualquier servidor DRA
Administrador ocasional del servicio de Ayuda técnica	Consola Web	Cualquier servidor DRA

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, Azure Active Directory, etc.).
- **Gestión de cuentas y recursos:** permite a los administradores asistentes de DRA ver y gestionar objetos delegados de dominios y servicios conectados desde la consola de delegación y configuración.

Consola Web

La consola Web es una interfaz de usuario basada en la Web que proporciona acceso rápido y fácil a los administradores asistentes para ver y gestionar objetos delegados de dominios y servicios conectados. Los administradores pueden personalizar el aspecto y el uso de la consola Web para incluir marcas empresariales y propiedades de objeto personalizadas.

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:

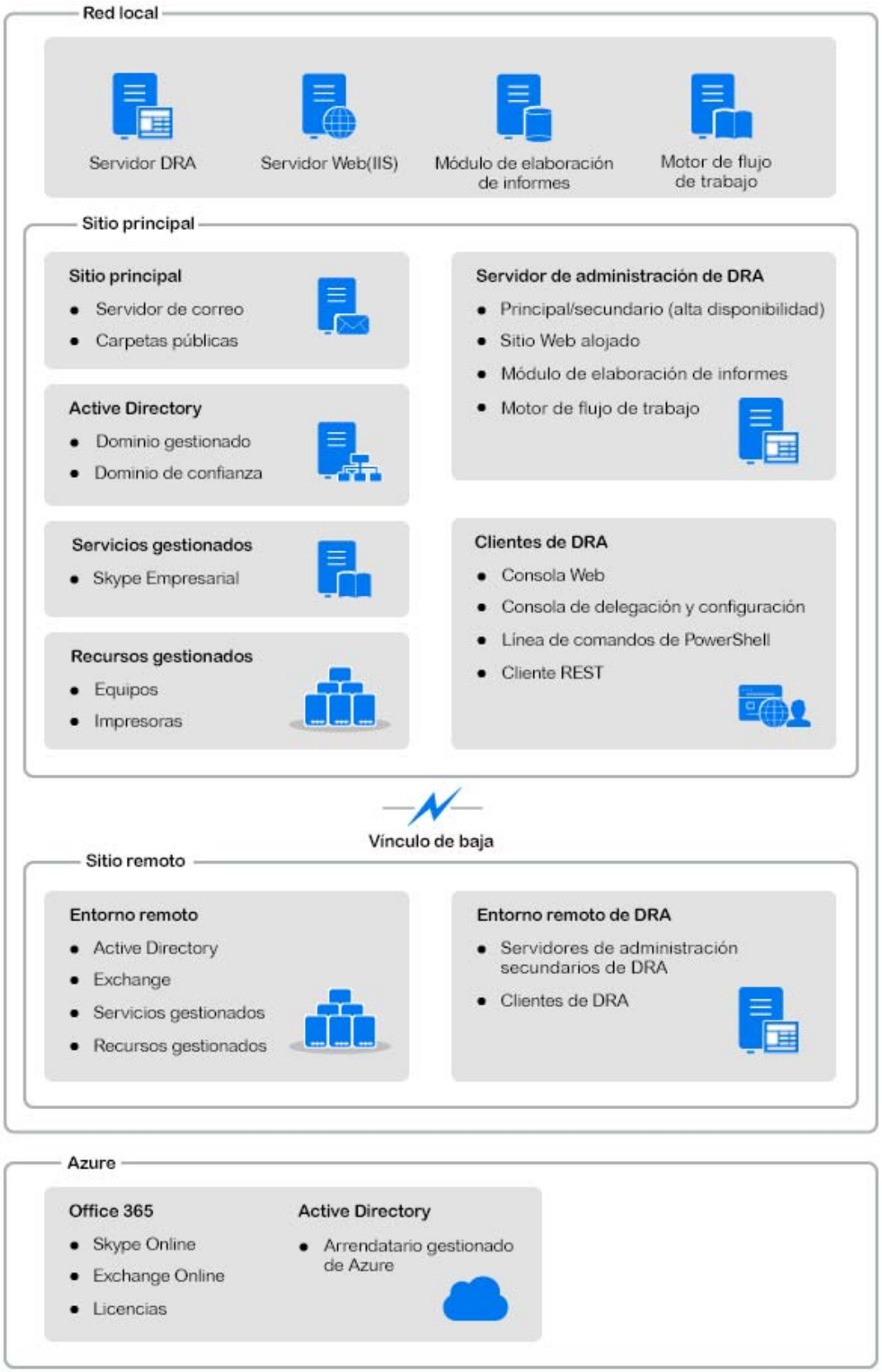
- Informes de recursos de objetos de Active Directory
- Informes de datos de objetos de Active Directory
- Informes de resumen de Active Directory
- Informes de configuración de DRA
- Informes de configuración de Exchange
- Informes de Office 365 Exchange Online
- Informes detallados de tendencia de 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 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.

Arquitectura del producto



II 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.

3 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	8 CPU/núcleos a 2,0 GHz	16 GB	120 GB
Consola Web de DRA	2 CPU/núcleos a 2,0 GHz	8 GB	100 GB
Módulo de elaboración de informes de DRA	4 CPU/núcleos a 2,0 GHz	16 GB	100 GB
Servidor de flujo de trabajo de DRA	4 CPU/núcleos a 2,0 GHz	16 GB	120 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)" (Reservar toda la memoria de invitado (Todo bloqueado).
- 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 (**).

Tablas de componentes:

- "Servidores de administración de DRA" en la página 20
- "Servidor REST de DRA" en la página 22
- "Consola Web (IIS)" en la página 22
- "Consola de delegación y administración de DRA" en la página 23
- "Servidor de flujo de trabajo" en la página 23

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*.
TCP 50000 *	Bidireccional	Servidores de administración de DRA	Réplica de atributos y comunicación entre el servidor DRA y AD LDS. (LDAP)
TCP 50001 *	Bidireccional	Servidores de administración de DRA	Réplica de atributos SSL (AD LDS)
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

Protocolo y puerto	Dirección	Destino	Uso
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 todas las instancias de Exchange Server 2013 local y posteriores (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).
TCP 443, 5986 y 5985	Saliente	Microsoft PowerShell	cmdlets nativos de PowerShell (HTTPS) y acceso remoto a PowerShell.
TCP 5984	Host local	Servidores de administración de DRA	Acceso de IIS al servicio de réplica para admitir asignaciones temporales de grupos.
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.
TCP 8898	Bidireccional	Servidores de administración de DRA	Comunicación del servicio de réplica de DRA entre servidores DRA para asignaciones temporales de grupos
TCP 636	Saliente	Controladores de dominio de Microsoft Active Directory	Gestión de objetos de Active Directory (LDAP SSL).

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* (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* (DCOM).
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.

Protocolo y puerto	Dirección	Destino	Uso
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 del producto de Directory and Resource Administrator.

Sistema gestionado	Requisitos previos
Azure Active Directory	Para habilitar la administración de Azure, debe instalar los siguientes módulos de PowerShell: ◆ Skype Empresarial Online https://www.microsoft.com/es-es/download/details.aspx?id=39366 ◆ Versión 2.0.2.4 de Azure Active Directory V2 (AzureAD) o posterior ◆ Versión 5.8.2 de AzureRM.Profile o posterior Se requieren PowerShell 5.1 o el módulo más reciente para instalar los nuevos módulos de PowerShell de Azure.
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online
Skype Empresarial	◆ Microsoft Skype Empresarial 2015
Historial de cambios	◆ Change Guardian 5.1 o posterior
Bases de datos	◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server 2017 ◆ Microsoft SQL Server 2019

Sistema gestionado	Requisitos previos
Navegadores Web	◆ Microsoft Internet Explorer 11 ◆ Google Chrome ◆ Mozilla Firefox
Automatización de flujos de trabajo	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016

Requisitos del servidor de administración de DRA, la consola Web y las extensiones REST

Los componentes de DRA requieren el software y las cuentas siguientes:

- "Requisitos de software" en la página 25
- "Dominio del servidor" en la página 27
- "Requisitos de la cuenta" en la página 28
- "Cuentas de acceso de DRA con privilegios mínimos" en la página 29

Requisitos de software

Componente	Requisitos previos
Destino de instalación	**Sistema operativo de NetIQ Administration Server:**
Sistema operativo	◆ Microsoft Windows Server 2012 R2, 2016 y 2019 **Nota:** El servidor también debe ser un miembro de un dominio de Microsoft Active Directory local admitido. **Interfaces de DRA:** ◆ Microsoft Windows Server 2012 R2, 2016 y 2019 ◆ Microsoft Windows 8.1 (x86 y x64) y 10 (x86 y x64)
Instalador	◆ Microsoft .NET Framework 4.6.2 y posterior

Componente	Requisitos previos
Servidor de administración	**Directory and Resource Administrator:** ◆ Microsoft .NET Framework 4.6.2 y posterior ◆ Microsoft Visual C++ 2013 Redistributable Packages (x64) y 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 ◆ Módulo Microsoft Internet Information Services URL Rewrite ◆ Enrutamiento de solicitud de aplicaciones de Microsoft Internet Information Services **Administración de Microsoft Office 365/Exchange Online:** ◆ Módulo Windows Azure Active Directory para Windows PowerShell ◆ Skype Empresarial Online y Módulo de Windows PowerShell Para obtener más información, consulte Plataformas compatibles.
Interfaz de usuario	**Interfaces de DRA:** ◆ Microsoft .NET Framework 4.6.2 ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 y x86)
Servicio de host de DRA	◆ Microsoft .NET Framework 4.6.2 ◆ Servidor de administración de DRA
Servicio y puesto final REST de DRA	◆ Microsoft .NET Framework 4.6.2
Extensiones de PowerShell	◆ Microsoft .NET Framework 4.6.2 ◆ PowerShell 5.1 o posterior

Componente	Requisitos previos
Consola Web de DRA	**Servidor Web:** ◆ Microsoft .NET Framework 4.x > Servicios WCF > Activación HTTP ◆ Microsoft Internet Information Server 8.0, 8.5 y 10 ◆ Módulo Microsoft Internet Information Services URL Rewrite ◆ Enrutamiento de solicitud de aplicaciones de Microsoft Internet Information Services **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

Dominio del servidor

Componente	Sistemas operativos
Servidor DRA	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

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.	◆ Para los 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).
		◆ Se debe seleccionar una de las siguientes pestañas Cuenta > **Opciones de cuenta** para el usuario de la cuenta del servicio de DRA si instala DRA en un servidor mediante la metodología STIG:
		  ◆ Cifrado AES de Kerberos de 128 bits
		  ◆ Cifrado AES de Kerberos de 256 bits
		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.
		◆ Para obtener más información sobre cómo configurar una cuenta de servicio gestionado de grupos para DRA, consulte: "Configuración de servicios de DRA para una cuenta de servicio gestionado de grupos".

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 DRA desde clientes remotos. Solo es necesario si se utiliza el cliente pesado o la consola de delegación y configuración. **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: Utilice ADSI Edit para otorgar a la cuenta de acceso al dominio los siguientes permisos de Active Directory en el nivel de dominio superior para los siguientes tipos de objetos descendientes:

- Control TOTAL de los objetos de builtInDomain
- Control TOTAL de los objetos de equipo
- Control TOTAL de los objetos de punto de conexión
- Control TOTAL de los objetos de contacto
- Control TOTAL de los objetos de contenedor
- Control TOTAL de los objetos de grupo
- Control TOTAL de los objetos de InetOrgPerson
- Control TOTAL de los objetos de MsExchDynamicDistributionList
- Control TOTAL de los objetos de MsExchSystemObjectsContainer
- Control TOTAL de los objetos de unidad administrativa
- Control TOTAL de los objetos de impresora
- Control TOTAL de los objetos de publicFolder
- Control TOTAL de los objetos de carpeta compartida
- Control TOTAL de los objetos de usuario

Otorgue a la cuenta de acceso al dominio los siguientes permisos de Active Directory en el nivel de dominio superior para este objeto y todos los objetos descendientes:

- Permitir creación de objetos de equipo.
- Permitir creación de objetos de contacto.
- Permitir creación de objetos de contenedor.
- Permitir creación de objetos de grupo.
- Permitir creación de objetos de MsExchDynamicDistributionList.

- Permitir creación de objetos de unidad administrativa.
- Permitir creación de objetos de publicFolders.
- Permitir creación de objetos de carpeta compartida.
- Permitir creación de objetos de usuario.
- Permitir supresión de objetos de equipo.
- Permitir supresión de objetos de contacto.
- Permitir supresión de contenedor.
- Permitir supresión de objetos de grupo.
- Permitir supresión de objetos de InetOrgPerson.
- Permitir supresión de objetos de MsExchDynamicDistributionList.
- Permitir supresión de objetos de unidad administrativa.
- Permitir supresión de objetos de publicFolders.
- Permitir supresión de objetos de carpeta compartida.
- Permitir supresión de objetos de usuario.

Nota

- Por defecto, algunos objetos de contenedor integrados de Active Directory no heredan los permisos del nivel superior del dominio. Por este motivo, los objetos requieren que se habilite la herencia o que se establezcan los permisos explícitos.
- Si el servidor REST no está instalado en el mismo servidor que el servidor de administración de DRA, la cuenta del servicio REST en ejecución debe tener control total sobre el servidor REST de Active Directory. Por ejemplo, defina el control TOTAL en `CN=DRARestServer,CN=System,DC=myDomain,DC=com`.

Cuenta de acceso a Exchange: para gestionar los objetos de Microsoft Exchange local, asigne la función de gestión administrativa a la cuenta de acceso a Exchange y esta al grupo Operadores de cuentas.

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

Cuenta de acceso de arrendatario de Azure: asigne los siguientes permisos de Azure Active Directory a la cuenta de acceso de arrendatario de Azure:

- Grupos de distribución
- Destinatarios de correo
- Creación de destinatarios de correo

- Creación de grupos de seguridad y pertenencia a ellos
- (Opcional) Administrador de Skype Empresarial

  Si desea gestionar Skype Empresarial Online, asigne el poder Administrador de Skype Empresarial a la cuenta de acceso de arrendatario de Azure.
- Administrador de usuarios

Permisos de la cuenta de servicio de administración de NetIQ:

- Administradores locales
- Otorgue la cuenta de anulación de privilegios mínimos "Permiso completo" en las carpetas compartidas o las carpetas DFS donde se aprovisionan los directorios principales.
- **Gestión de recursos**: para gestionar los recursos publicados en un dominio de Active Directory gestionado, se debe otorgar a la cuenta de acceso al dominio permisos de administración local en esos recursos.

Después de la instalación de DRA: Después de que los dominios necesarios se añadan o estén siendo administrados por DRA, ejecute los siguientes comandos:

- 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>`
- Para delegar permiso en la "NetIQReceyleBin OU" de la carpeta de instalación de DRA:

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

Acceso remoto a SAM: asigne controladores de dominio o servidores miembros gestionados por DRA para habilitar las cuentas que se enumeran a continuación en la configuración de GPO a fin de que puedan realizar consultas remotas en la base de datos del Administrador de cuentas de seguridad (SAM). La configuración debe incluir la cuenta de servicio de DRA.

Acceso de red: restrinja clientes con permiso para realizar llamadas remotas a SAM.

Para acceder a esta opción, realice lo siguiente:

1. Abra la consola de gestión de directivas de grupo en el controlador de dominio.
2. Expanda **Dominios** > **[controlador de dominio]** > **Objetos de directiva de grupo** en el árbol de nodos.
3. Haga clic con el botón derecho en **Directiva predeterminada de controladores de dominio** y seleccione **Editar** para abrir el editor de GPO de esta directiva.
4. Expanda **Configuración del equipo** > **Directivas** > **Configuración de Windows** > **Configuración de seguridad** > **Directivas locales** en el árbol de nodo del editor de GPO.
5. Haga doble clic en **Acceso de red: evitar que clientes con permiso realicen llamadas remotas a SAM** en el panel de directivas y seleccione **Definir esta configuración de directiva**.
6. Haga clic en **Editar seguridad** y habilite la opción **Permitir** para el acceso remoto. Añada la cuenta de servicio de DRA si no se ha incluido aún como usuario o parte del grupo de administradores.
7. Aplique los cambios. Esto añadirá el descriptor de seguridad `O:BAG:BAD:(A;;RC;;;BA)` a la configuración de directivas.

Para obtener más información, consulte el artículo 7023292 de Knowledge Base.

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 R2, 2016 y 2019
NetIQ Reporting Center (v3.2)	**Base de datos:** ◆ Microsoft SQL Server 2016, 2017 y 2019 ◆ 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:** ◆ Necesario para ejecutar el programa de instalación de NRC. ◆ Necesario también en el servidor principal de DRA para la configuración de los servicios de elaboración de informes de DRA. **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 usar la utilidad de comprobación de estado para instalar la licencia adquirida. También se incluye una clave de licencia de prueba (TrialLicense.lic) en el paquete de instalación que permite 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.

4 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.

El paquete de servidor DRA presenta las siguientes funciones:

- **Servidor de administración:** almacena los datos de configuración (entorno, acceso delegado y directiva), ejecuta tareas de operador y automatización, y audita la actividad de todo el sistema. Contiene las siguientes funciones:
  - **Kit de recursos del archivo de registro:** permite ver la información de auditoría.
  - **SDK de DRA:** proporciona los guiones de ejemplo de ADSI y le ayuda a crear sus propios guiones.
- **Servicio y puestos finales REST:** 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.
- **Interfaces de usuario:** la interfaz del cliente Web utilizada principalmente por los administradores asistentes, que también incluye opciones de personalización.
  - **Proveedor ADSI:** le permite crear sus propios guiones de directivas.
  - **Interfaz de línea de comandos:** permite realizar operaciones de DRA.
  - **Delegación y configuración:** permite a los administradores del sistema acceder a las funciones de configuración y administración de DRA. Además, permite especificar y asignar de forma granular el acceso a las tareas y los recursos gestionados a los administradores asistentes.
  - **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:** la interfaz del cliente Web utilizada principalmente por los administradores asistentes, que también incluye opciones de personalización.

Para obtener información acerca de la instalación de consolas y clientes de línea de comandos de DRA en varios equipos, consulte Instalación de los clientes de DRA.

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 admin.	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.
Instalar DRA	Haga clic en **Instalar DRA** y, a continuación, en **Siguiente**para ver las opciones de instalación. **Nota:** Para ejecutar la instalación más adelante, acceda a la ubicación en la que se han extraído los medios de instalación (consulte el kit de instalación) y ejecute `Setup.exe`.
Instalación por defecto	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: **Servidor de administración** ◆ Kit de recursos del archivo de registro ◆ SDK de DRA **Servicios REST** **Interfaces de usuario** ◆ Proveedor ADSI ◆ Interfaz de línea de comandos ◆ Delegación y configuración ◆ Extensiones de PowerShell ◆ Consola Web
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 los conjuntos de varios maestros, consulte “Configuración del conjunto de varios maestros” en la *Guía del administrador de Directory and Resource Administrator*.

Paso	Detalles
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, la consola Web y las extensiones REST.
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.
Especificar la ubicación de la base de datos de réplica de DRA	◆ Especifique la ubicación del archivo de la base de datos de réplica de DRA y el puerto del servicio de réplica. ◆ Especifique el certificado SSL que desea utilizar para las comunicaciones seguras con la base de datos a través de IIS y especifique el puerto de réplica.
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.
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. Para obtener más información, consulte la "Utilidad de comprobación de estado" en la *Guía del administrador de DRA*.

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:

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 la interfaz de usuario 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 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).

Instalación del módulo de elaboración de informes de DRA

El módulo de elaboración de informes de DRA requiere que instale el archivo DRAReportingSetup.exe desde el kit de instalación de DRA de NetIQ.

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 cumplir el requisito previo del instalador del producto DRA.
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 DRA`ReportingSetup.exe` para instalar el componente de gestión para la integración del módulo de elaboración de informes de DRA.

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. Para obtener más información sobre NetIQ Reporting Center, consulte *Reporting Center Guide* (Guía de Reporting Center) en el sitio Web de documentación.
Aceptar el acuerdo de licencia (EULA)	Acepte los términos del acuerdo de licencia de usuario final para completar la ejecución de la instalación.

5 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” en la *Guía del administrador de DRA*.

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 administradores asistentes dependen de cada MMS. Si la mayoría de los administradores asistentes dependen de servidores o conjuntos de servidores específicos, actualice primero esos servidores durante las horas de menor actividad.
- Determine los administradores asistentes que necesitan la consola de delegación y configuración. Puede obtener esta información de una de las siguientes formas:
  - Consulte los administradores asistentes asociados a los grupos de administradores asistentes integrados.
  - Consulte los administradores asistentes 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 administradores asistentes acerca de sus planes de actualización de las interfaces de usuario.
- Determine los administradores asistentes que deben conectarse al servidor de administración principal. Estos administradores asistentes deben actualizar los equipos cliente una vez que actualice el servidor de administración principal.

  Informe a estos administradores asistentes acerca de sus planes para actualizar los servidores de administración y las 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.

Importante

- Si la versión anterior de DRA tiene instalada la consola de gestión de cuentas y recursos (ARM), esta se eliminará durante la actualización.
- Al actualizar el servidor DRA desde una versión DRA 9.x, se eliminan todos los arrendatarios gestionados de DRA. Para seguir utilizando estos arrendatarios mediante Azure, debe añadirlos después de la actualización. Para obtener información sobre cómo añadir arrendatarios, consulte “Creación de una aplicación de Azure y adición de un arrendatario de Azure” en la *Guía del administrador de DRA*.
- Debido a que Exchange 2010 no es compatible con DRA 10, Exchange se inhabilita cuando se actualiza desde DRA 9.x. Para continuar realizando operaciones de Exchange después de la actualización, inhabilite y vuelva a habilitar la opción **Enable Exchange Policy** (Habilitar directiva de Exchange) en la consola de delegación y configuración. Deben "aplicarse" los dos cambios para restablecer la directiva.

  Para obtener información sobre esta configuración de directivas, consulte “Habilitación de Microsoft Exchange” en la *Guía del administrador de DRA*.

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 del administrador asistente). 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.

Pasos	Detalles
Sincronizar el MMS	Sincronice los conjuntos de servidores para que cada servidor de administración contenga la configuración y los ajustes de seguridad más recientes.
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..
Convertir gMSA en cuentas de usuario de DRA	*Opcional:* si utiliza una cuenta de servicio gestionado por el grupo (gMSA) para la cuenta de servicio de DRA, cambie la cuenta de gMSA a una cuenta de usuario de DRA antes de actualizar. Después de la actualización, deberá cambiar de nuevo la cuenta a gMSA.

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.

Temas anteriores a la actualización:

- "Reserva de un servidor de administración local para la ejecución de una versión anterior de DRA" en la página 43
- "Sincronización del conjunto de servidores con la versión anterior de DRA" en la página 44
- "Copia de seguridad del registro del servidor de administración" en la página 45

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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 Abra la consola de delegación y configuración y expanda **Configuration Management** (Gestión de configuraciones).

3 Haga clic en **Servidores de administración**.

4 En el panel de la derecha, seleccione el servidor de administración principal adecuado para este conjunto de servidores.

5 Haga clic en **Propiedades**.

6 En la pestaña Programación de sincronización, haga clic en **Actualizar ahora**.

7 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.

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

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.

Importante: La instalación de actualización de DRA realiza los siguientes cambios cuando actualiza el servidor DRA de una versión DRA 9.x a una versión DRA 10.x:

- Mueve las configuraciones de usuario del servidor de UCH y Automatización del flujo de trabajo de la consola Web a la consola de delegación y configuración
- Elimina el componente Web anterior del servidor.
- Elimina todos los arrendatarios gestionados.

  Para obtener información acerca de la adición de arrendatarios, consulte "Gestión de arrendatarios" en la *Guía del administrador de DRA*.
- Si ha instalado la consola de gestión de cuentas y recursos de una versión anterior y, al actualizar a una versión DRA 10.x, se eliminará esta consola.
- Durante una actualización de MMS, el servidor principal se actualiza primero y, a continuación, los servidores secundarios. Para realizar correctamente la réplica de las asignaciones temporales de grupos en el servidor secundario, ejecute la **programación de sincronización de varios maestros** manualmente o espere a la ejecución programada.
- Debido a que Exchange 2010 no es compatible con DRA 10, Exchange se inhabilita cuando se actualiza desde DRA 9.x. Para continuar realizando operaciones de Exchange después de la actualización, inhabilite y vuelva a habilitar la opción **Enable Exchange Policy** (Habilitar directiva de Exchange) en la consola de delegación y configuración. Deben "aplicarse" los dos cambios para restablecer la directiva.

  Para obtener información sobre esta configuración de directivas, consulte *Habilitación de Microsoft Exchange*.

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.

Pasos	Detalles
Actualizar el servidor principal	Actualice el servidor de administración principal del MMS adecuado. Para obtener más información, consulte Actualización del servidor de administración principal.
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. Para obtener más información, consulte Instalación de un servidor de administración secundario local para la versión actual de DRA.
Implantar las interfaces de usuario	Implante las interfaces de usuario en los administradores asistentes. Para obtener más información, consulte Implantación de las interfaces de usuario de DRA
Actualizar los servidores secundarios	Actualice los servidores de administración secundarios del MMS. Para obtener más información, consulte Actualización de los servidores de administración secundarios.
Actualizar el módulo de elaboración de informes de DRA	Actualice el módulo de elaboración de informes de DRA. Para obtener más información, consulte Actualización del módulo de elaboración de informes.
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.
Añadir arrendatarios de Azure *(posterior a la actualización)*	(*Opcional, posterior a la actualización)* Si, antes de la actualización, gestionaba arrendatarios de Azure, estos se eliminarán durante la actualización. Deberá añadir de nuevo esos arrendatarios y ejecutar una actualización completa de la memoria caché de cuentas desde la consola de delegación y configuración. Para obtener más información, consulte "Gestión de arrendatarios" en la *Guía del administrador de DRA*.

Temas sobre la actualización del servidor:

- “Actualización del servidor de administración principal” en la página 47
- “Instalación de un servidor de administración secundario local para la versión actual de DRA” en la página 48
- “Implantación de las interfaces de usuario de DRA” en la página 49
- “Actualización de los servidores de administración secundarios” en la página 49

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 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 más instrucciones e información de actualización, consulte las *Notas de la versión de Directory and Resource Administrator*.

Antes de actualizar, informe a los administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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 administradores asistentes 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, el proveedor ADSI o PowerShell, 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 administradores asistentes 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 administradores asistentes.

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 del administrador asistente, 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 administradores asistentes que utilizan este servidor que instalen las interfaces de usuario adecuadas, como la consola Web.
3. Repita los pasos 1 y 2 anteriores hasta que actualice por completo el MMS.

Antes de actualizar, informe a los administradores asistentes 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 administradores asistentes 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 del administrador asistente ejecuten interfaces de usuario actualizadas, desconecte todos los servidores restantes con la versión anterior de DRA.

Actualización del 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 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 DRA`ReportingSetup.exe` desde el kit de instalación y siga las instrucciones del asistente de instalación.
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.

III 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.

6 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.
Configurar los controladores de dominio y los servidores de administración	Configure el equipo cliente que ejecuta la consola de delegación y configuración para cada controlador de dominio y servidor de administración. Para obtener más información, consulte Configuración del controlador de dominio y el servidor de administración.
Configurar los servicios de DRA para una gMSA	*Opcional:* configure los servicios de DRA para una cuenta de servicio gestionado de grupos (gMSA). Para obtener más información, consulte Configuración de los servicios de DRA para una cuenta de servicio gestionado de grupos.

7 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 la licencia adquirida. Si es necesario, se proporciona también una clave de licencia de prueba (`TrialLicense.lic`) con el paquete de instalación que permite gestionar un número ilimitado de cuentas de usuario y buzones durante 30 días.

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.

8 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 "Configuración del almacenamiento en caché" en la *Guía del administrador de Directory and Resource Administrator*.

---

9 Adición de subárboles gestionados

Puede añadir subárboles gestionados o ausentes de dominios específicos de Microsoft Windows después de instalar el servidor de administración. Estas funciones se ejecutan en la consola de delegación y configuración desde el nodo **Configuration Management** (Gestión de configuraciones) > **Managed Domains** (Dominios gestionados). 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 "Utilidad Objetos eliminados" en la *Guía del administrador de Directory and Resource Administrator*.

Para obtener más información sobre la configuración de la cuenta de acceso, consulte "Especificar cuentas de acceso al dominio" en la *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 "Configuración del almacenamiento en caché" en la *Guía del administrador de Directory and Resource Administrator*.

---

10 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.

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 pertenencia a grupo debe incluir la cuenta de servicio de DRA, todos los administradores asistentes y la cuenta utilizar para gestionar el servicio REST, el host y los servicios de administración de DRA.

Para configurar el grupo Usuarios COM distribuidos:

1. Entre en un equipo cliente de Administración 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**.

11 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 al **Panel de Control** > **Sistema y seguridad**.
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.

12 Configuración de los servicios de DRA para una cuenta de servicio gestionado de grupos

Si es necesario, puede utilizar una cuenta de servicio gestionado de grupos (gMSA) para los servicios de DRA. Para obtener más información sobre el uso de gMSA, consulte la referencia de Microsoft *Group Managed Service Accounts Overview* (Descripción general de las cuentas de servicios gestionados de grupos). En esta sección, se explica cómo configurar DRA para una cuenta de servicio gestionado de grupos después de añadir previamente la cuenta a Active Directory.

Importante: No utilice la gMSA como una cuenta de servicio al instalar DRA.

Para configurar el servidor de administración principal de DRA para una gMSA:

1. Añada la gMSA como miembro de los grupos siguientes:
   - Grupo Administradores locales en el servidor DRA
   - Grupo AD LDS en el dominio gestionado de DRA
2. Cambie la cuenta de inicio de sesión a la gMSA en las propiedades de servicio para cada uno de los servicios siguientes:
   - Servicio de administración de NetIQ
   - Servicio de auditoría de DRA de NetIQ
   - Servicio de caché de DRA de NetIQ
   - Servicio del núcleo de DRA de NetIQ
   - Servicio de host de DRA de NetIQ
   - Archivo de registro de DRA de NetIQ
   - Servicio de réplica de DRA de NetIQ
   - Servicio REST de DRA de NetIQ
   - Servicio de Skype de DRA de NetIQ
3. Reinicie todos los servicios.

Para configurar un servidor de administración secundario de DRA para una gMSA:

1. Instale el servidor secundario.
2. En el servidor principal, asigne la función **Configurar servidores y dominios** a la ActiveView **Servidores de administración y dominios gestionados** para la cuenta de servicio del servidor secundario.
3. En el servidor principal, añada un nuevo servidor secundario y especifique la cuenta de servicio del servidor secundario.

4. Añada el gMSA al grupo de administradores locales en el servidor de administración secundario de DRA.
5. En el servidor secundario, cambie la cuenta de inicio de sesión de todos los servicios de DRA a la gMSA y, a continuación, vuelva a iniciar los servicios de DRA.