ManageEngine
ADManager Plus

Permisos necesarios para la cuenta de AD configurada en ADManager Plus

www.manageengine.com/latam/ad-manager/

Tabla de contenido

Para llevar a cabo las operaciones deseadas de gestión e informes de Active Directory (AD), ADManager Plus debe contar con los permisos necesarios. Para ello, ingrese las credenciales de una cuenta de usuario a la que se hayan concedido los permisos necesarios en la pestaña Administración de ADManager Plus de la sección Ajustes del dominio.

Para modificar los Grupos privilegiados, debe iniciar sesión con una cuenta de usuario que sea miembro del Grupo de administradores. Si no desea utilizar una cuenta de administrador de dominio, puede iniciar sesión con una cuenta de usuario a la que se hayan concedido privilegios suficientes para realizar las operaciones necesarias.

Las siguientes secciones contienen los privilegios mínimos que se deben asignar a una cuenta de usuario para realizar la operación requerida.

Gestión de usuarios

Esta sección ofrece una explicación detallada sobre los permisos necesarios para crear, modificar y eliminar cuentas de usuario.

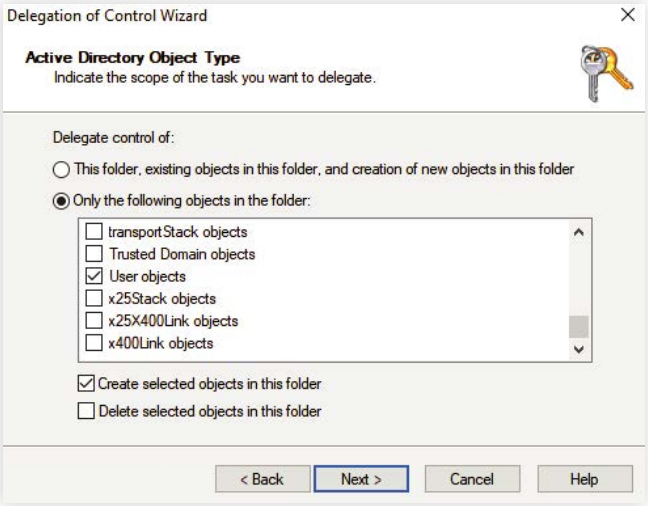
Operación: Crear usuarios

Permisos necesarios:

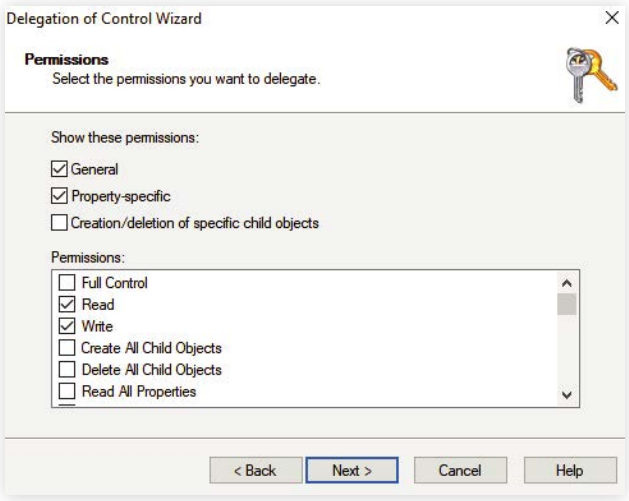
- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener los permisos Leer y Escribir en todos los objetos de usuario de la OU requerida.

Pasos para conceder los permisos necesarios para crear una cuenta de usuario.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers.**
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de usuario**. También seleccione la opción **Crear los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad**.
7. En la sección de permisos, seleccione los permisos **Leer** y **Escribir** y haga clic en **Siguiente** como se indica en la siguiente imagen



8. Haga clic en **Finalizar**.

Operación: Modificar usuarios

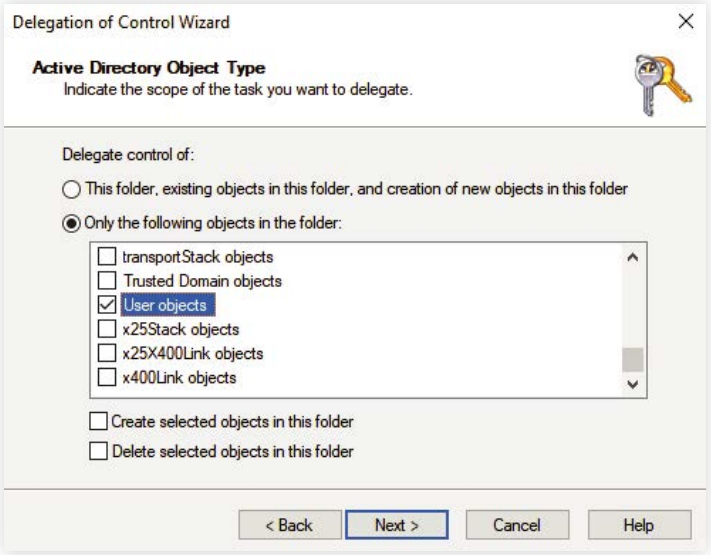
Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas

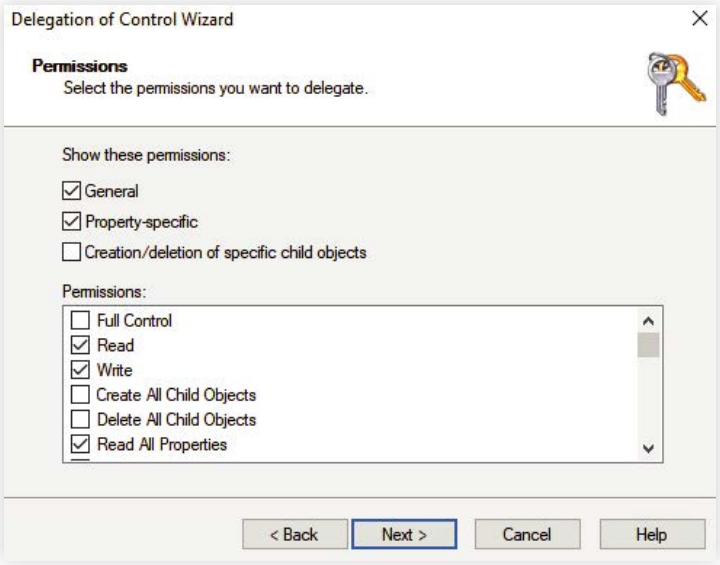
- Debe tener los permisos Leer, Escribir, Leer todas las propiedades en todos los objetos de usuario de la OU requerida.

Pasos para conceder los permisos necesarios para modificar una cuenta de usuario.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers**.
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y seleccione la opción **Objetos de usuario** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad**.
7. En la sección de permisos, seleccione los permisos **Leer, Escribir y Leer todas las propiedades** y haga clic en **Siguiente** como se indica en la siguiente imagen.



8. Haga clic en **Finalizar**.

Operación: Eliminar usuarios

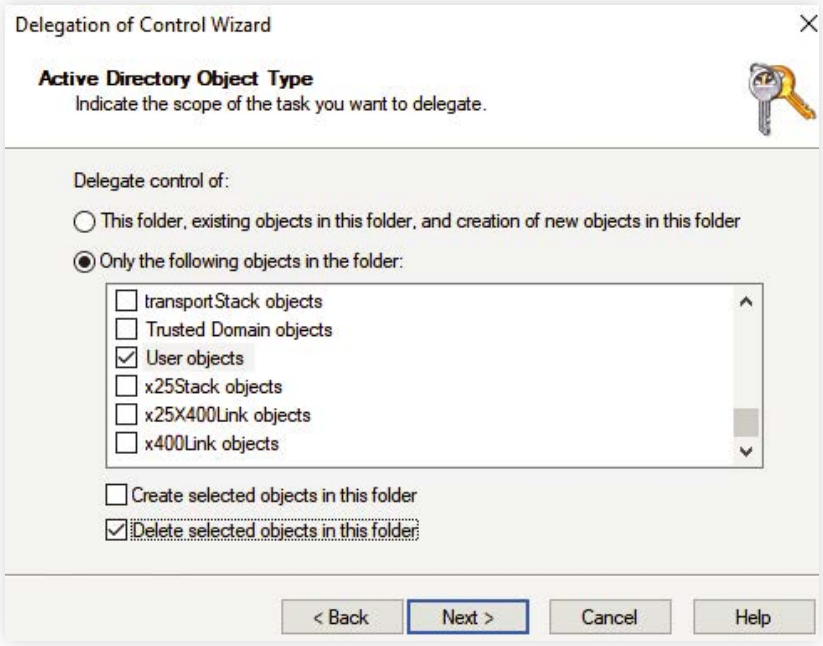
Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas

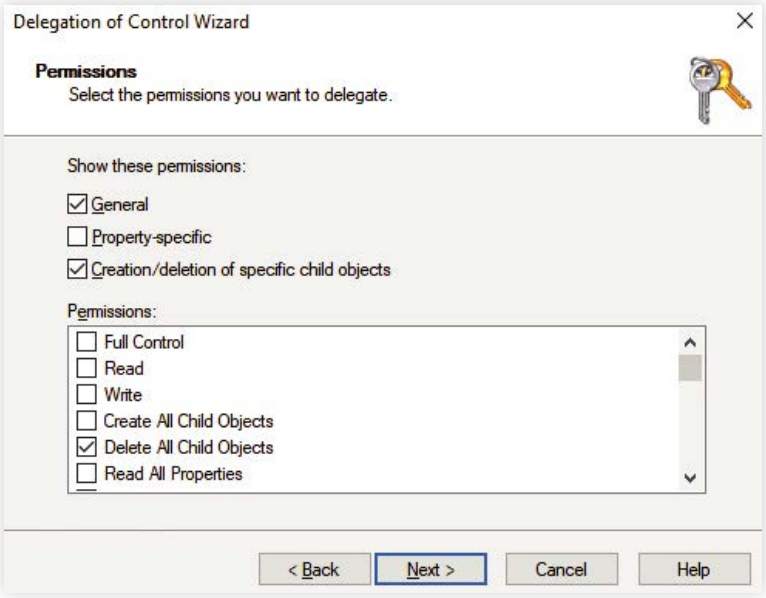
- Debe tener el permiso para Eliminar todos los objetos secundarios en todos los objetos de usuario de la OU requerida.

Pasos para conceder los permisos necesarios para eliminar una cuenta de usuario.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers**.
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de usuario**. También seleccione la opción **Eliminar los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Crear/eliminar objetos secundarios específicos**.
7. En la sección de permisos, seleccione el permiso **Eliminar todos los objetos secundarios** y haga clic en **Siguiente** como se indica en la siguiente imagen.



8. Haga clic en **Finalizar**.

Operación: Restaurar usuarios

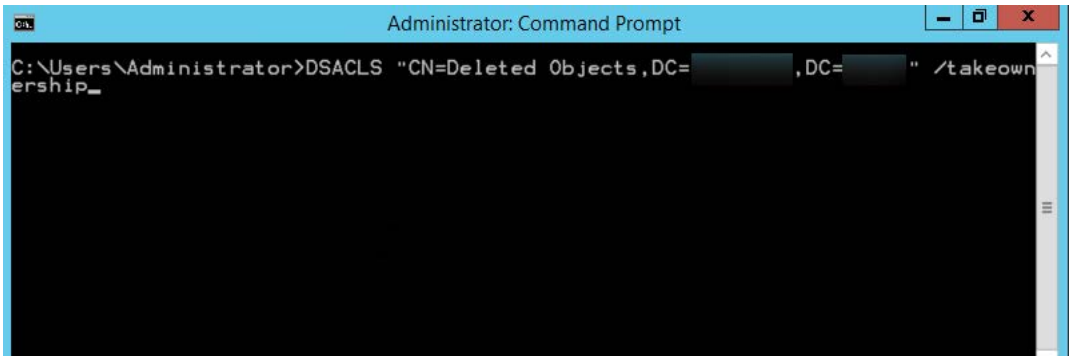
Permisos necesarios:

- Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de Administradores de dominio.
- La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.

Pasos para conceder los permisos necesarios para restaurar un usuario de AD eliminado

Cualquier objeto eliminado de AD se almacena en el contenedor de objetos eliminados y se puede restaurar antes de que finalice su periodo de vida útil. Para restaurar un objeto de AD eliminado, los no administradores deben tener permiso suficiente para acceder a este contenedor.
Para conceder los permisos necesarios:

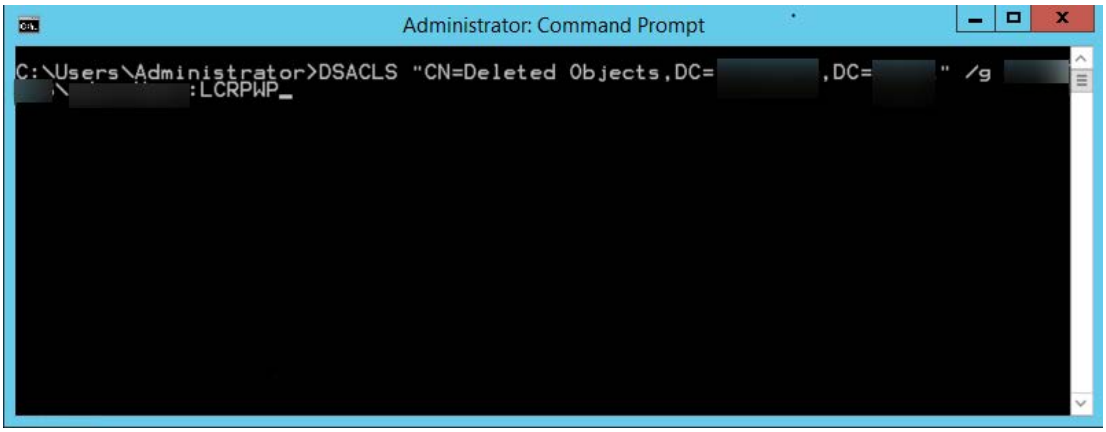
1. Inicie sesión en su **controlador de dominio** e inicie el símbolo del sistema de las herramientas ADAM.
2. Especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=**admanagerplus**,DC=**com**" /takeownership



Nota:

- Cada dominio de un bosque tendrá su propio contenedor de objetos eliminados, por lo que es esencial especificar el nombre de dominio del contenedor de objetos eliminados para el que desea modificar los permisos.
- Sustituya admanagerplus y com por los componentes de su dominio.

3. Para conceder permiso a una entidad de seguridad para acceder al contenedor de objetos eliminados, especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP



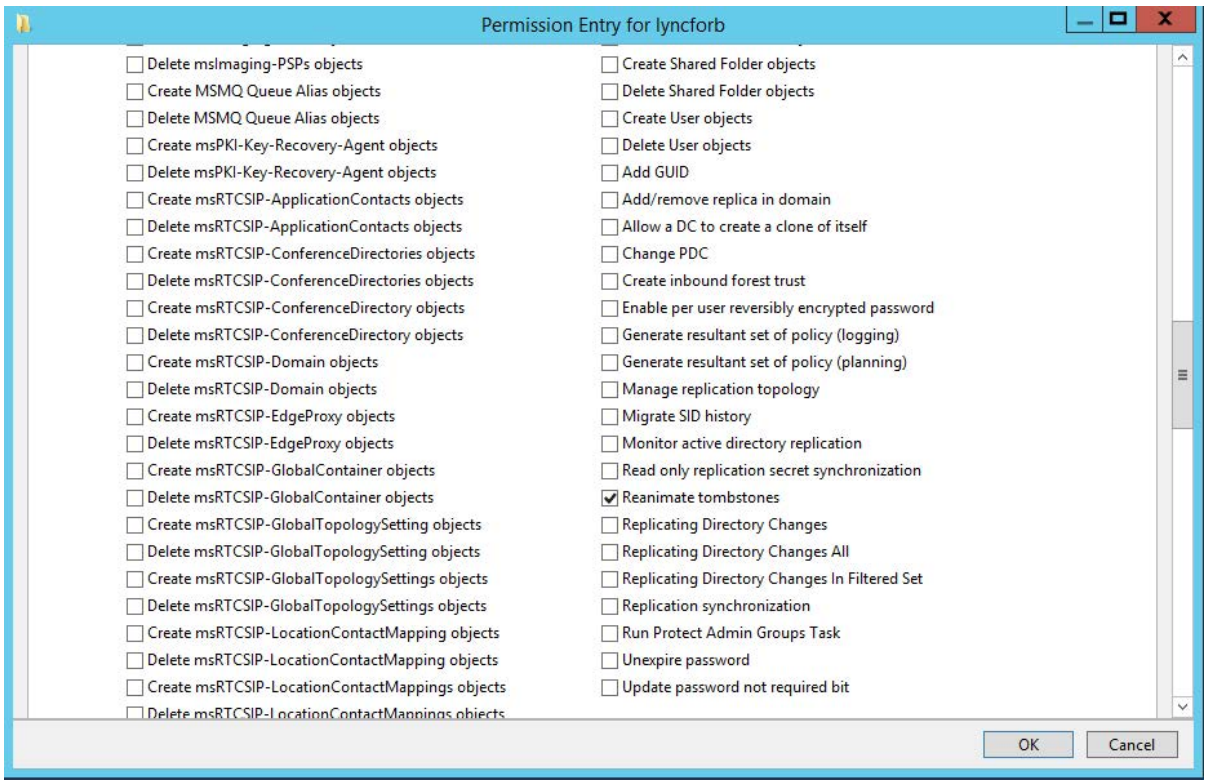
Nota: Sustituya "LukeJohnson" por el principal de seguridad de su elección.

4. A continuación, conéctese al contexto de nomenclatura predeterminado, haga clic derecho en la raíz del dominio y seleccione **Propiedades.**

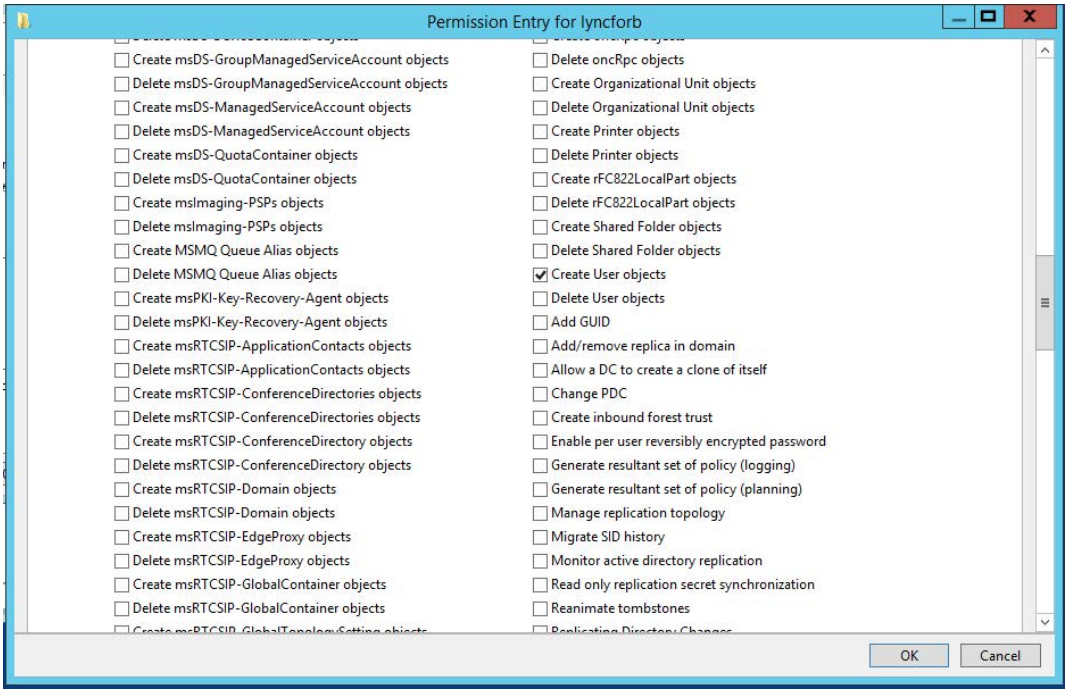
5. Vaya a la pestaña **Seguridad** y haga clic en **Avanzado.**

6. Añada el usuario o grupo y seleccione los siguientes derechos:

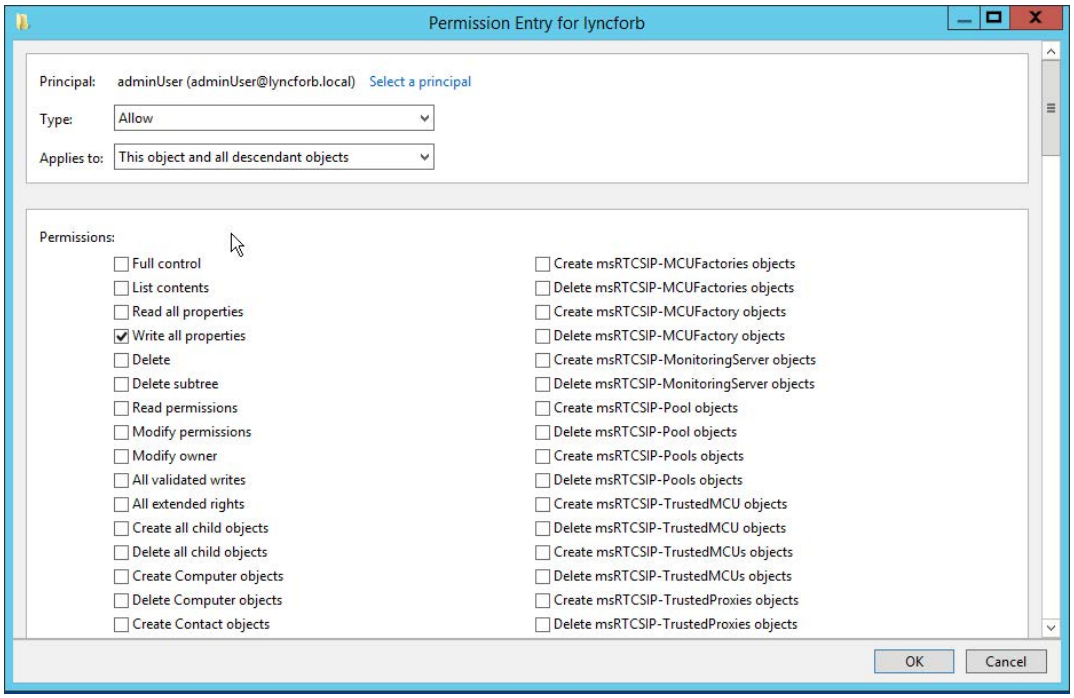
   a. Reanimate tombstones



b. Crear objetos de usuario.



c. Escribir todas las propiedades



Nota: Aplique el derecho Reanimate tombstones al objeto que se está protegiendo y a sus objetos descendientes.

7. Haga clic en **Aceptar**.

Nota: Sólo se pueden restaurar los objetos borrados después de delegar los permisos mencionados.

Mkyz0Ft jk iutzgizuy

Esta sección ofrece una explicación detallada sobre los permisos necesarios para crear, modificar y eliminar contactos en AD.

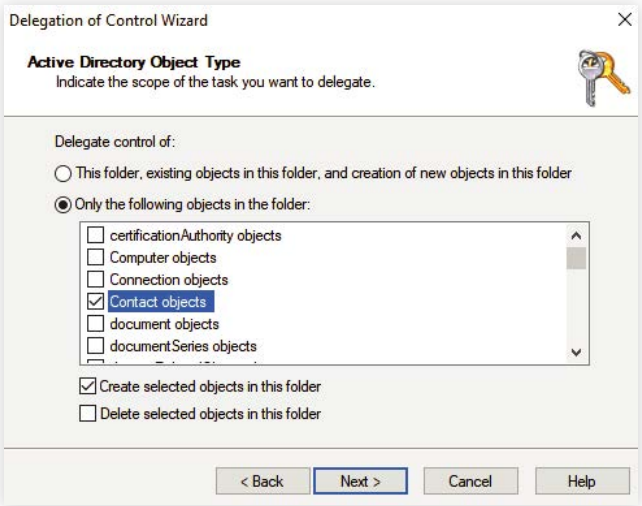
Uvkxgi0Ftg Crear contactos

Vkx s0yuy tkikygx0uyg

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener los permisos Leer y Escribir en todos los objetos de contacto de la OU requerida.

Vgyuy vgxg iut ikjkx ruy vkx s0yuy tkikygx0uy vgxg ixkgx {tg i{ktzg jk iutzgizu4

1. Inicie sesión en su controlador de dominio y ejecute **Giz0|k J0xkizux [ykxy gt j lusv{zkxy**.
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Jkrkmgx iutzxur**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Y0m{0ktzk**, añada la cuenta de usuario necesaria y haga clic en **Y0m{0ktzk**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de contacto.** También seleccione la opción **Crear los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen:



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad.**
7. En la sección de permisos, seleccione los permisos **Leer** y **Escribir** y haga clic en **Siguiente.**
8. Haga clic en **Finalizar.**

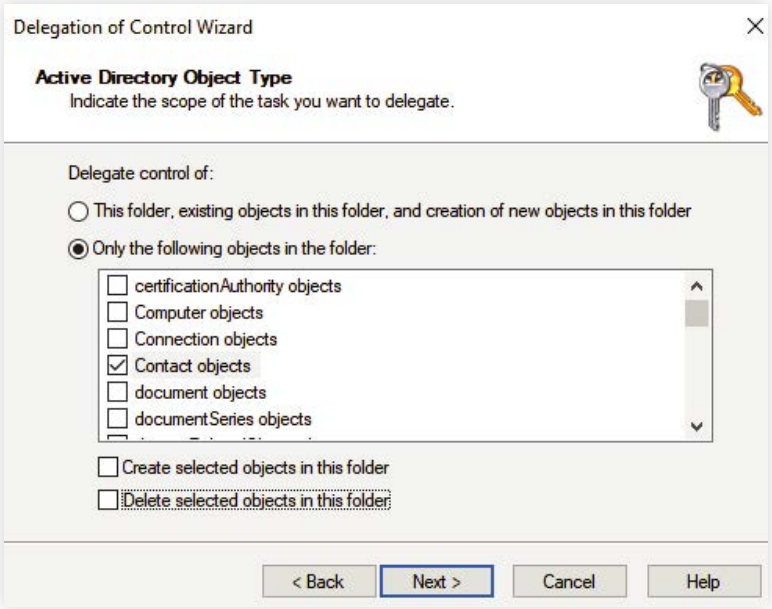
Operación: Modificar contactos

Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener los permisos Leer, Escribir, Leer todas las propiedades en todos los objetos de usuario de la OU requerida.

Pasos para conceder los permisos necesarios para modificar una cuenta de contacto.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers.**
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada para delegar**.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y seleccione la opción **Objetos de contacto** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente.** En la sección **Mostrar estos permisos**, seleccione las opciones **General y Específico de la propiedad.**
7. En la sección de permisos, seleccione los permisos **Leer, Escribir** y **Leer todas las propiedades** y haga clic en **Siguiente.**
8. Haga clic en **Finalizar.**

Operación: Eliminar contactos

Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener el permiso para Eliminar todos los objetos secundarios en todos los objetos de contacto de la OU requerida.

Pasos para conceder los permisos necesarios para eliminar una cuenta de contacto.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers**.
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de contacto**. También seleccione la opción **Eliminar los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen:

6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Crear/eliminar objetos secundarios específicos**.
7. En la sección de permisos, seleccione el permiso **Eliminar todos los objetos secundarios** y haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

Operación: Restaurar contactos

Permisos necesarios:

- Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de Administradores de dominio.

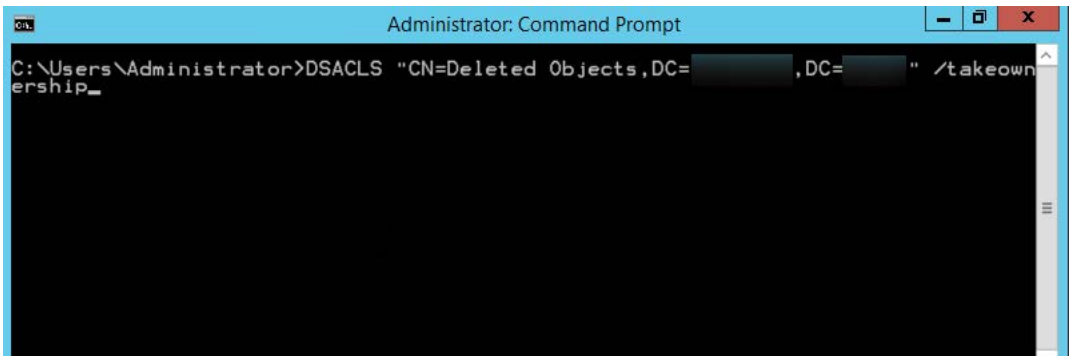
- La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.

Pasos para conceder los permisos necesarios para restaurar un contacto de AD eliminado

Cualquier objeto eliminado de AD se almacena en el contenedor de objetos eliminados y se puede restaurar antes de que finalice su periodo de vida útil. Para restaurar un objeto de AD eliminado, los no administradores deben tener permiso suficiente para acceder a este contenedor.
Para conceder los permisos necesarios:

1. Inicie sesión en su **controlador de dominio** e inicie el símbolo del sistema de las herramientas ADAM.

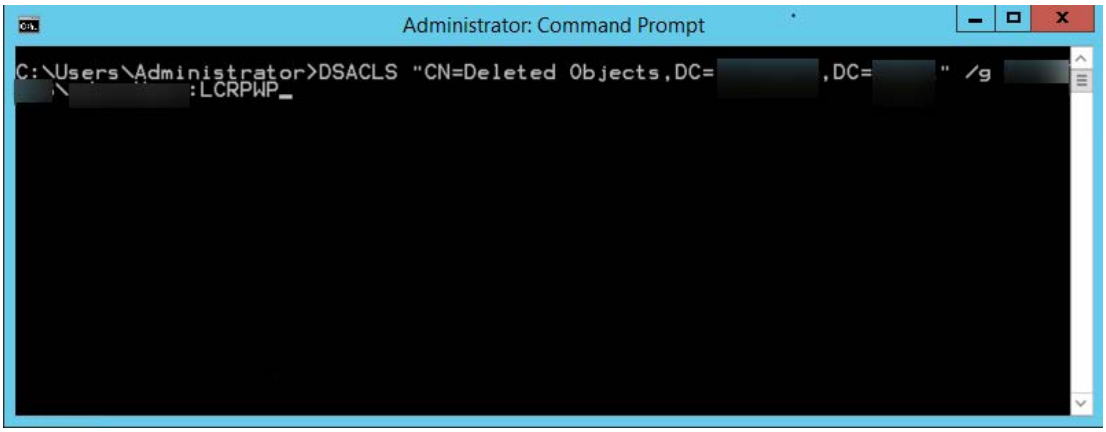
2. Especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=**admanagerplus**,DC=com" /takeownership



Nota:

- Cada dominio de un bosque tendrá su propio contenedor de objetos eliminados, por lo que es esencial especificar el nombre de dominio del contenedor de objetos eliminados para el que desea modificar los permisos.
- Sustituya admanagerplus y com por los componentes de su dominio.

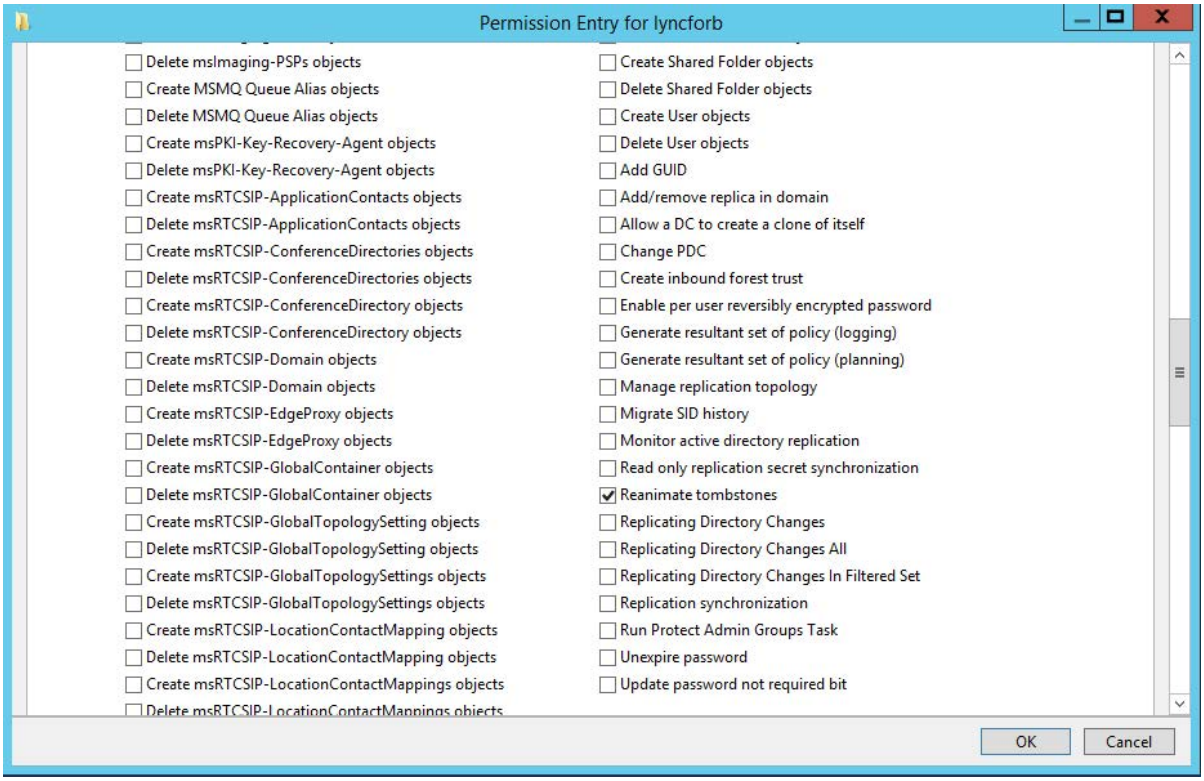
3. Para conceder permiso a una entidad de seguridad para acceder al contenedor de objetos eliminados, especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP



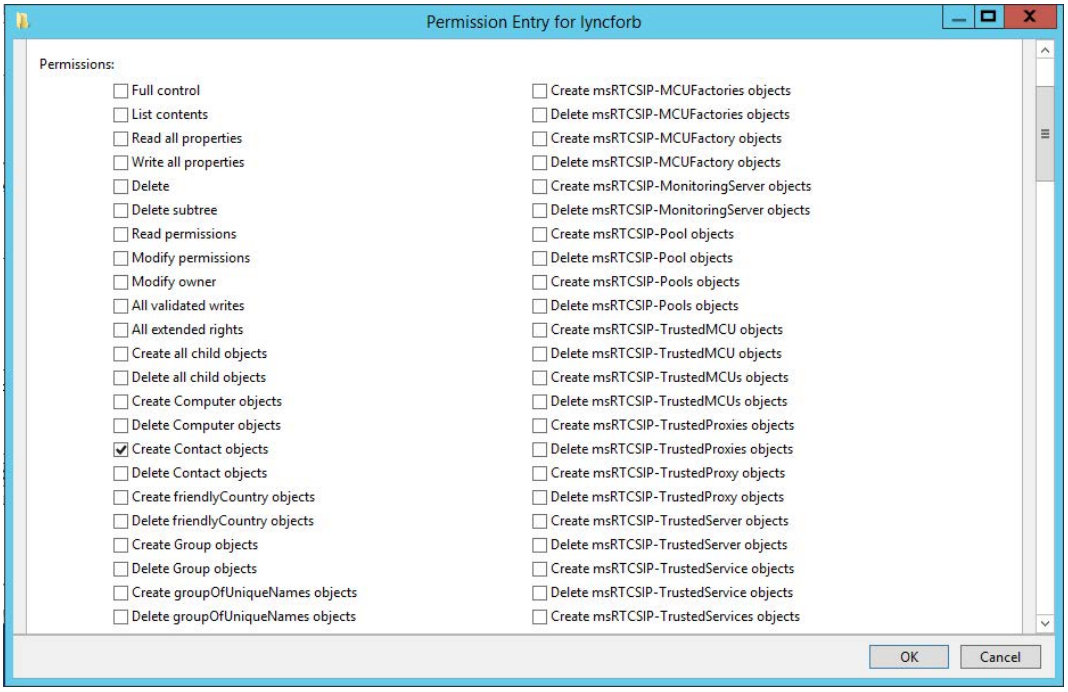
Nota: Sustituya "LukeJohnson" por el principal de seguridad de su elección.

1. A continuación, conéctese al contexto de nomenclatura predeterminado, haga clic derecho en la raíz del dominio y seleccione **Propiedades**.
2. Vaya a la pestaña **Seguridad** y haga clic en **Avanzado**.
3. Añada el usuario o grupo y seleccione los siguientes derechos:

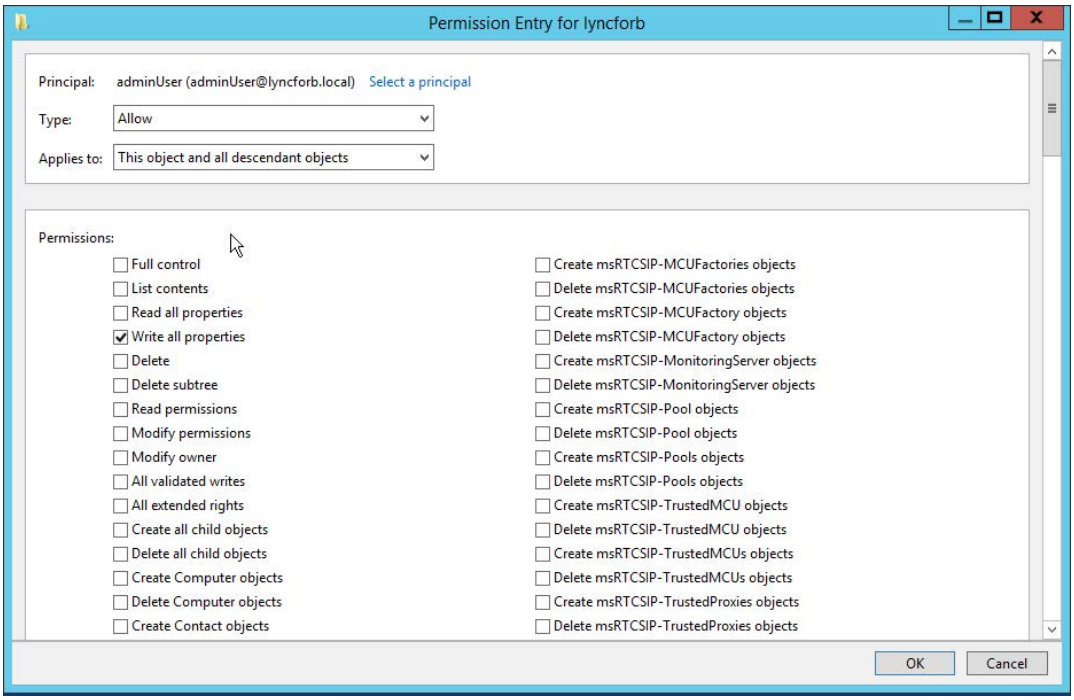
   a. Reanimate tombstones



b. Crear objetos de contacto



c. Escribir todas las propiedades



Nota: Aplique el derecho **Reanimate tombstones** al objeto que está protegiendo y a sus objetos descendientes.

7. Haga clic en **Aceptar.**

Nota: Sólo se pueden restaurar los objetos borrados después de delegar los permisos mencionados.

Gestión de equipos

Esta sección ofrece una explicación detallada sobre los permisos necesarios para crear, modificar y eliminar equipos en AD.

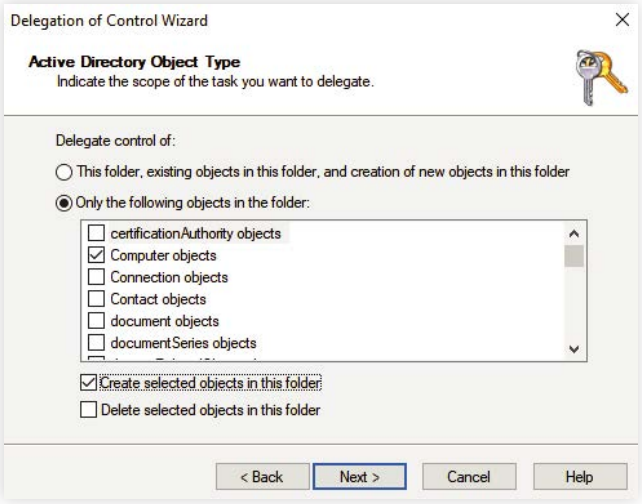
Operación: Crear equipos

Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener los permisos Leer y Escribir en todos los objetos de equipo de la OU requerida.

Pasos para conceder los permisos necesarios para crear una cuenta de equipo.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers.**
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegaciên de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de equipo.** También seleccione la opción **Crear los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos,** seleccione las opciones **General** y **Específico de la propiedad.**
7. En la sección de permisos, seleccione los permisos **Leer**, **Escribir** y haga clic en **Siguiente.**
8. Haga clic en **Finalizar**.

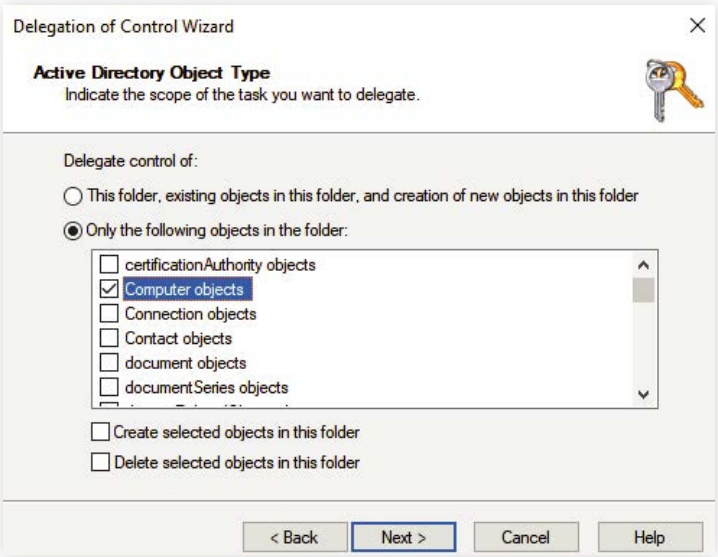
Operación: Modificar equipos

Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener los permisos Leer, Escribir, Leer todas las propiedades en todos los objetos de equipo de la OU requerida.

Pasos para conceder los permisos necesarios para modificar una cuenta de equipo.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers.**
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control.** Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y seleccione la opción **Objetos de equipo** como se indica en la siguiente imagen:



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad**.
7. En la sección de permisos, seleccione los permisos **Leer**, **Escribir** y **Leer todas las propiedades** y haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

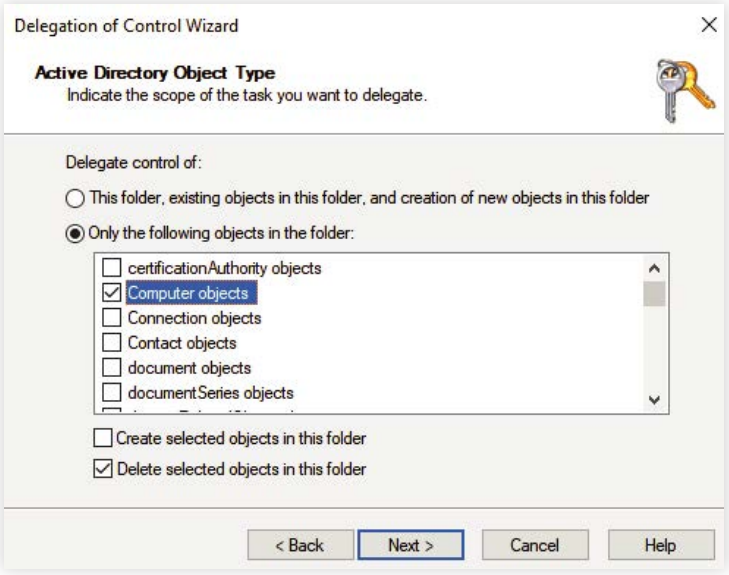
Operación: Eliminar equipos

Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener el permiso para Eliminar todos los objetos secundarios en todos los objetos de equipo de la OU requerida.

Pasos para conceder los permisos necesarios para eliminar una cuenta de equipo.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers**.
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control.** Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y seleccione la opción **Objetos de equipo** como se indica en la siguiente imagen:



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos,** seleccione las opciones **General** y **Crear/eliminar objetos secundarios específicos**.
7. En la sección de permisos, seleccione el permiso **Eliminar todos los objetos secundarios** y haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

Operación: Restaurar equipos

Permisos necesarios:

- Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de Administradores de dominio.

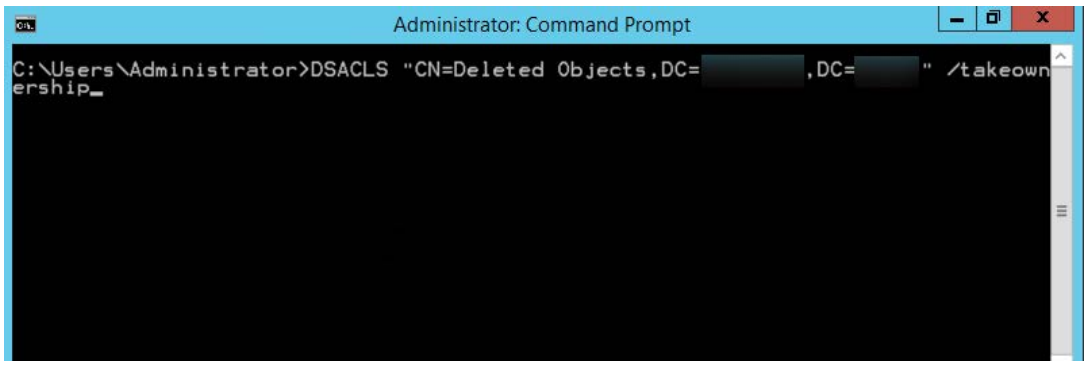
- La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.

Pasos para conceder los permisos necesarios para restaurar un equipo de AD eliminado

Cualquier objeto eliminado de AD se almacena en el contenedor de objetos eliminados y se puede restaurar antes de que finalice su periodo de vida útil. Para restaurar un objeto de AD eliminado, los no administradores deben tener permiso suficiente para acceder a este contenedor.

Para conceder los permisos necesarios:

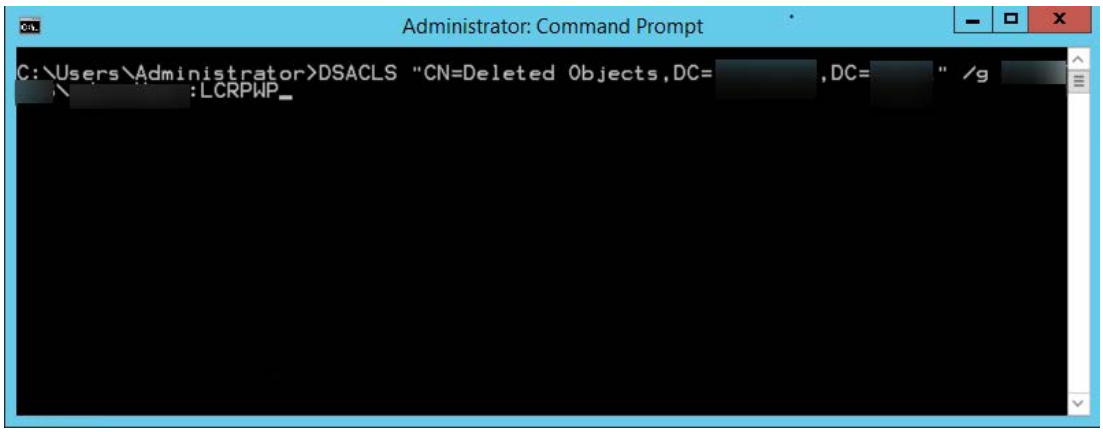
1. Inicie sesión en su **controlador de dominio** e inicie el símbolo del sistema de las herramientas ADAM.
2. Especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=**admanagerplus**,DC=**com**" /takeownership



Nota:

- Cada dominio de un bosque tendrá su propio contenedor de objetos eliminados, por lo que es esencial especificar el nombre de dominio del contenedor de objetos eliminados para el que desea modificar los permisos.
- Sustituya **admanagerplus** y **com** por los componentes de su dominio.

3. Para conceder permiso a una entidad de seguridad para acceder al contenedor de objetos eliminados, especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP

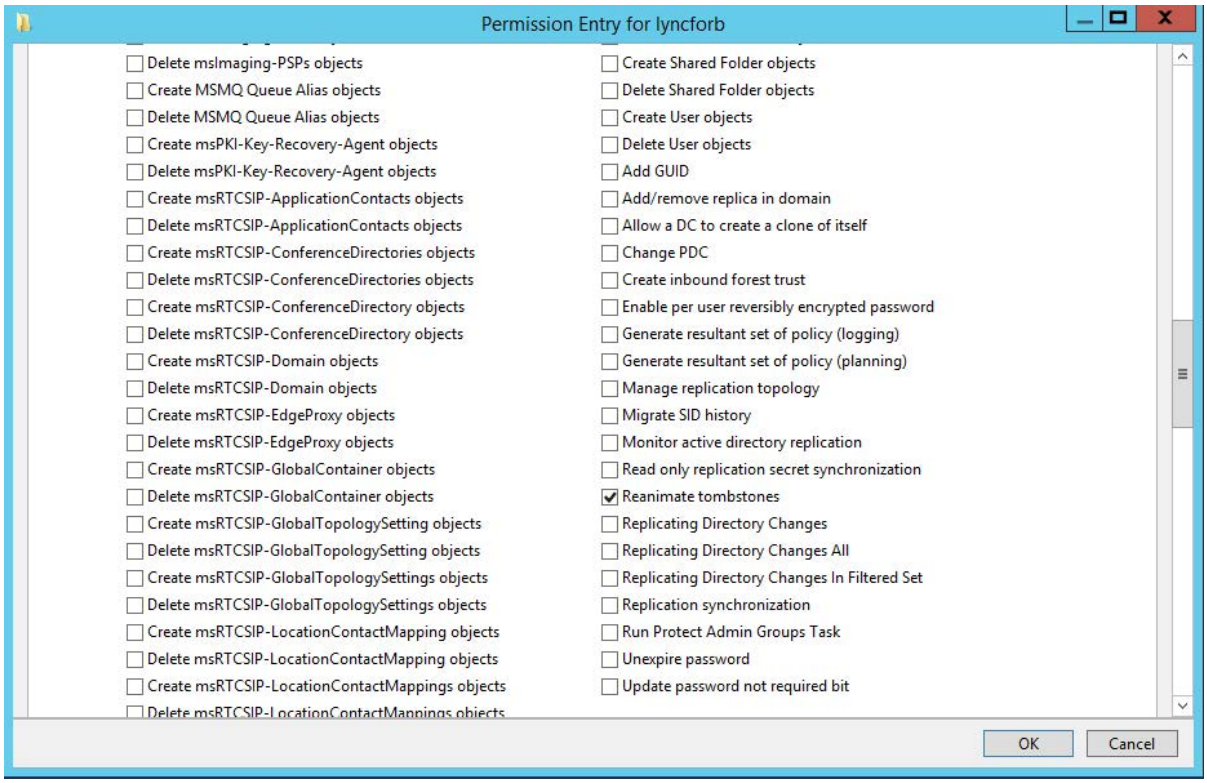


Nota: Sustituya "LukeJohnson" por el principal de seguridad de su elección.

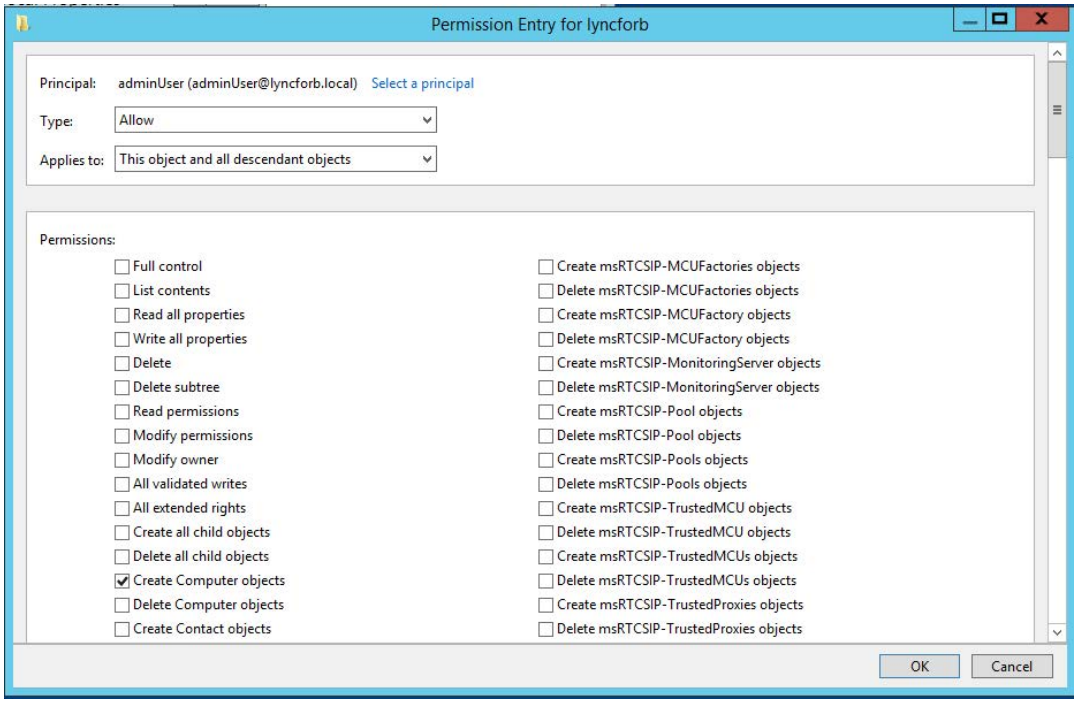
4. A continuación, conéctese al contexto de nomenclatura predeterminado, haga clic derecho en la raíz del dominio y seleccione **Propiedades**.

5. Vaya a la pestaña **Seguridad** y haga clic en **Avanzado**.

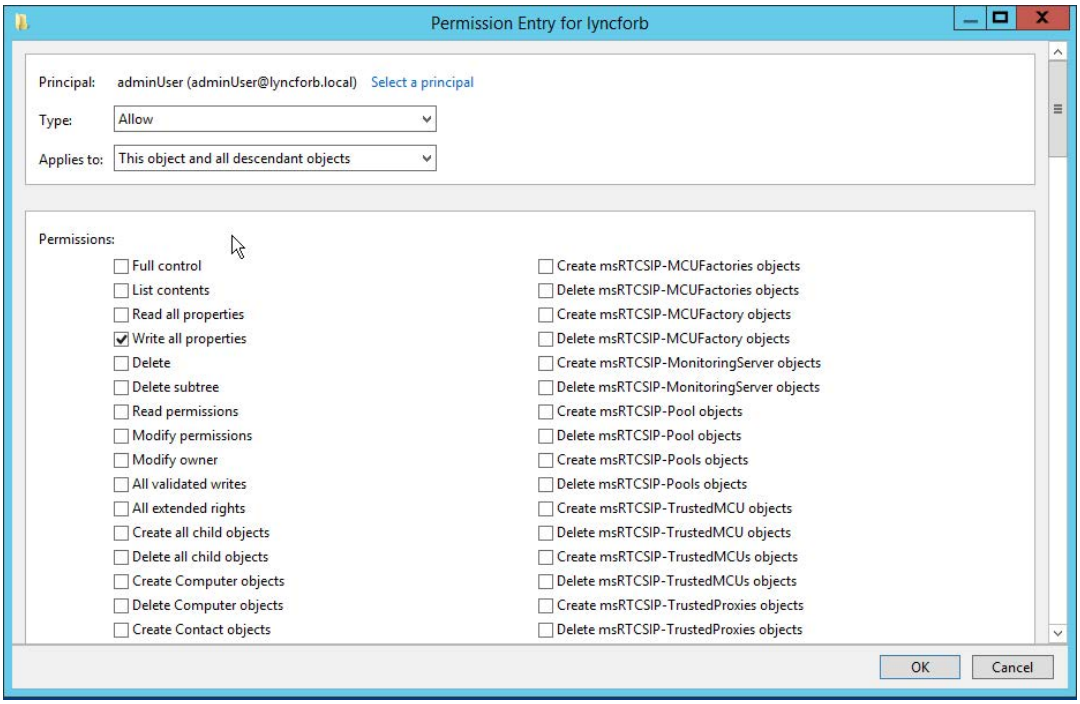
6. Añada el usuario o grupo y seleccione los siguientes derechos:
   a. Reanimate tombstones



b. Crear objetos de equipo



c. Escribir todas las propiedades



Nota: Aplique el derecho **Reanimate tombstones** al objeto que está protegiendo y a sus objetos descendientes.

7. Haga clic en **Aceptar**.

Nota: Sólo se pueden restaurar los objetos borrados después de delegar los permisos mencionados.

Gestión de grupos

Esta sección ofrece una explicación detallada sobre los permisos necesarios para crear, modificar y eliminar grupos en AD.

Operación: Crear grupos

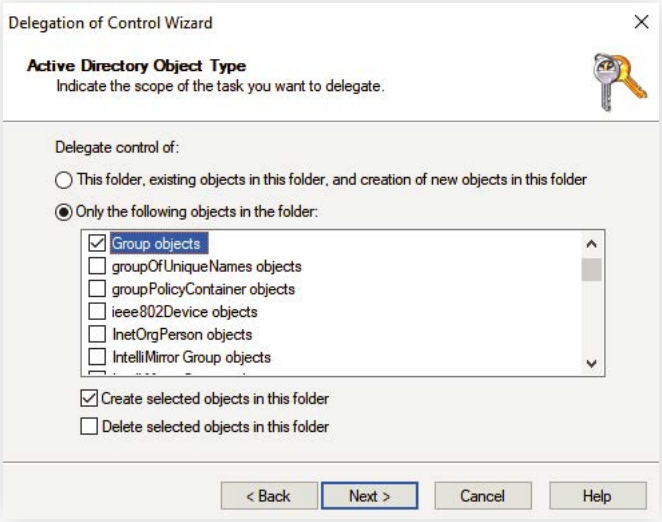
Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas

- Debe tener los permisos Leer y Escribir en todos los objetos de grupo de la OU requerida.

Pasos para conceder los permisos necesarios para crear grupos.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers.**
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control.** Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de grupo.** También seleccione la opción **Crear los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad.**
7. En la sección de permisos, seleccione los permisos **Leer** y **Escribir** y haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

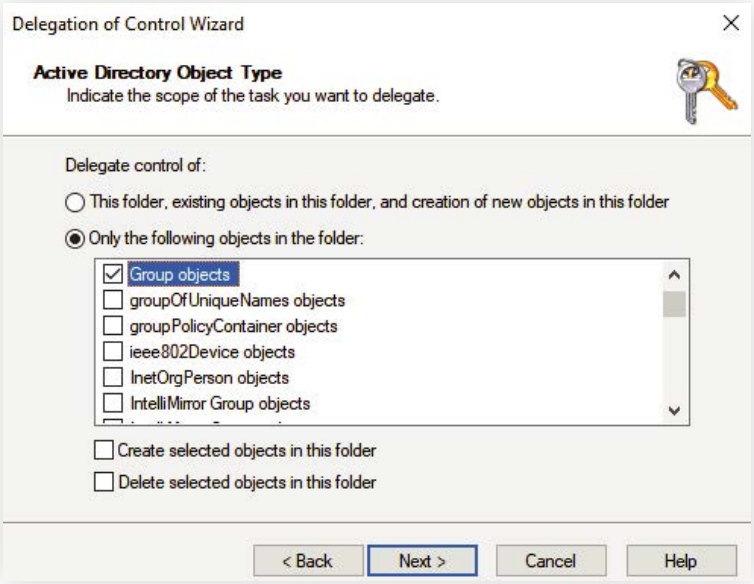
Operación: Modificar grupos

Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas
- Debe tener los permisos Leer, Escribir, Leer todas las propiedades en todos los objetos de grupo de la OU requerida.

Pasos para conceder los permisos necesarios para modificar grupos.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers**.
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y seleccione la opción **Objetos de grupo** como se indica en la siguiente imagen.



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad**.
7. En la sección de permisos, seleccione los permisos **Leer**, **Escribir** y **Leer todas las propiedades** y haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

Operación: Eliminar grupos

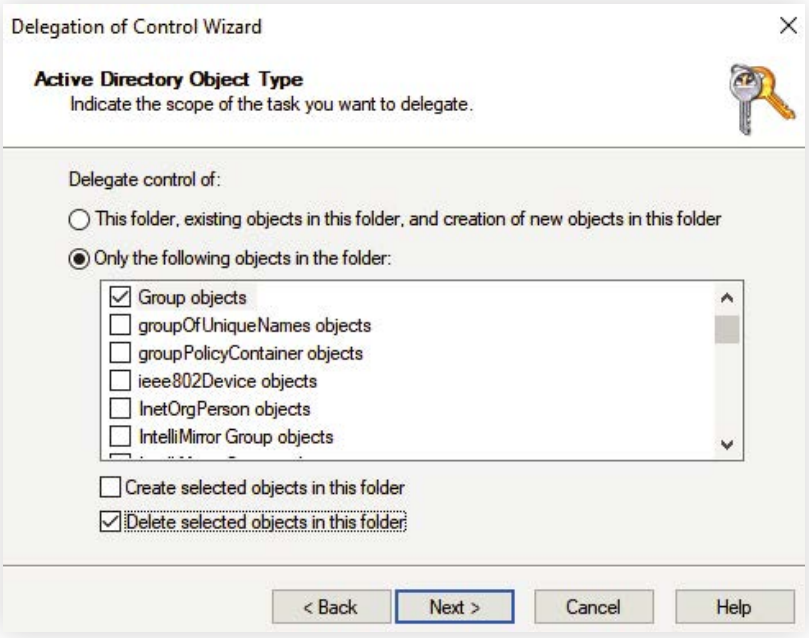
Permisos necesarios:

- Debe ser miembro del Grupo de operadores de cuentas

- Debe tener el permiso para Eliminar todos los objetos secundarios en todos los objetos de grupo de la OU requerida.

Pasos para conceder los permisos necesarios para eliminar grupos.

1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers.**
2. Localice y haga clic derecho en el dominio/OU para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**, añada la cuenta de usuario necesaria y haga clic en **Siguiente**.
4. Seleccione la opción **Crear una tarea personalizada** para delegar.
5. Seleccione la opción **Sólo los objetos en esta carpeta** y marque la casilla **Objetos de grupo**. También seleccione la opción **Eliminar los objetos seleccionados en esta carpeta** como se indica en la siguiente imagen:



6. Haga clic en **Siguiente**. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Crear/eliminar objetos secundarios específicos**.
7. En la sección de permisos, seleccione el permiso **Eliminar todos los objetos secundarios** y haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

Operación: Restaurar grupos

Permisos necesarios:

- Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de Administradores de dominio.

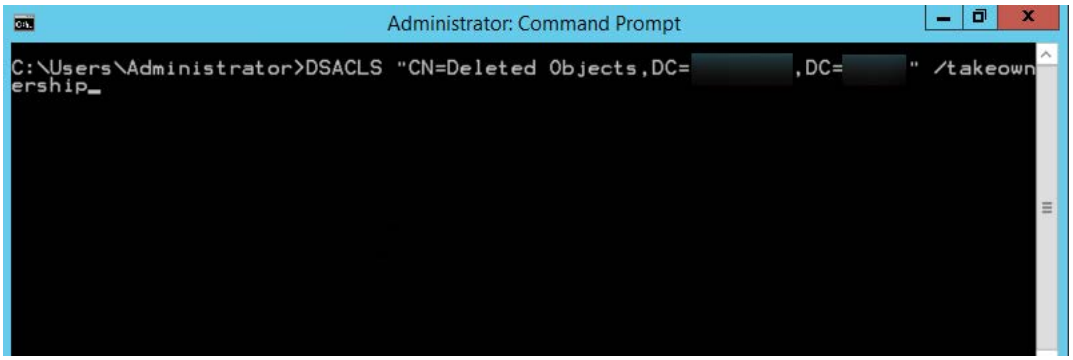
- La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.

Pasos para conceder los permisos necesarios para restaurar un grupo de AD eliminado

Cualquier objeto eliminado de AD se almacena en el contenedor de objetos eliminados y se puede restaurar antes de que finalice su periodo de vida útil. Para restaurar un objeto de AD eliminado, los no administradores deben tener permiso suficiente para acceder a este contenedor.

Para conceder los permisos necesarios:

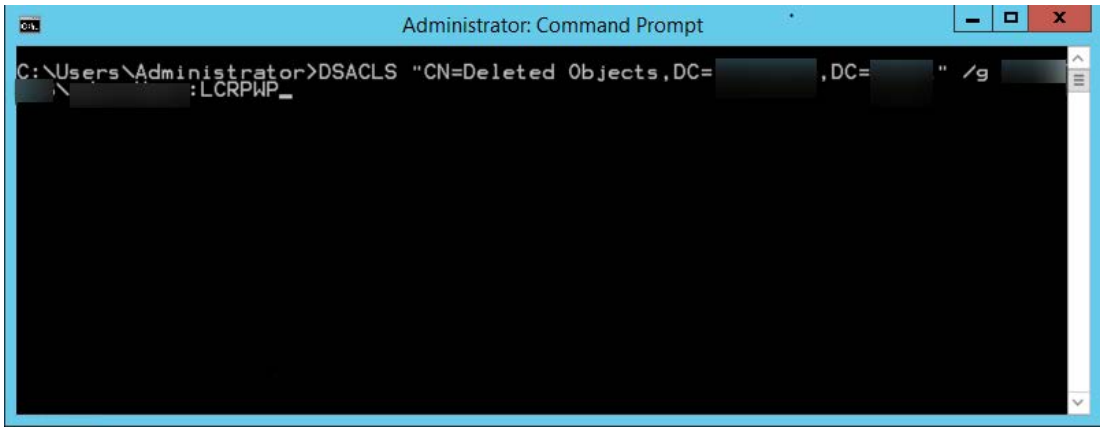
1. Inicie sesión en su controlador de dominio e inicie el símbolo del sistema de las herramientas ADAM.
2. Especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /takeownership



Nota:

- Cada dominio de un bosque tendrá su propio contenedor de objetos eliminados, por lo que es esencial especificar el nombre de dominio del contenedor de objetos eliminados para el que desea modificar los permisos.
- Sustituya admanagerplus y com por los componentes de su dominio..

3. Para conceder permiso a una entidad de seguridad para acceder al contenedor de objetos eliminados, especifique un comando con el siguiente formato: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP

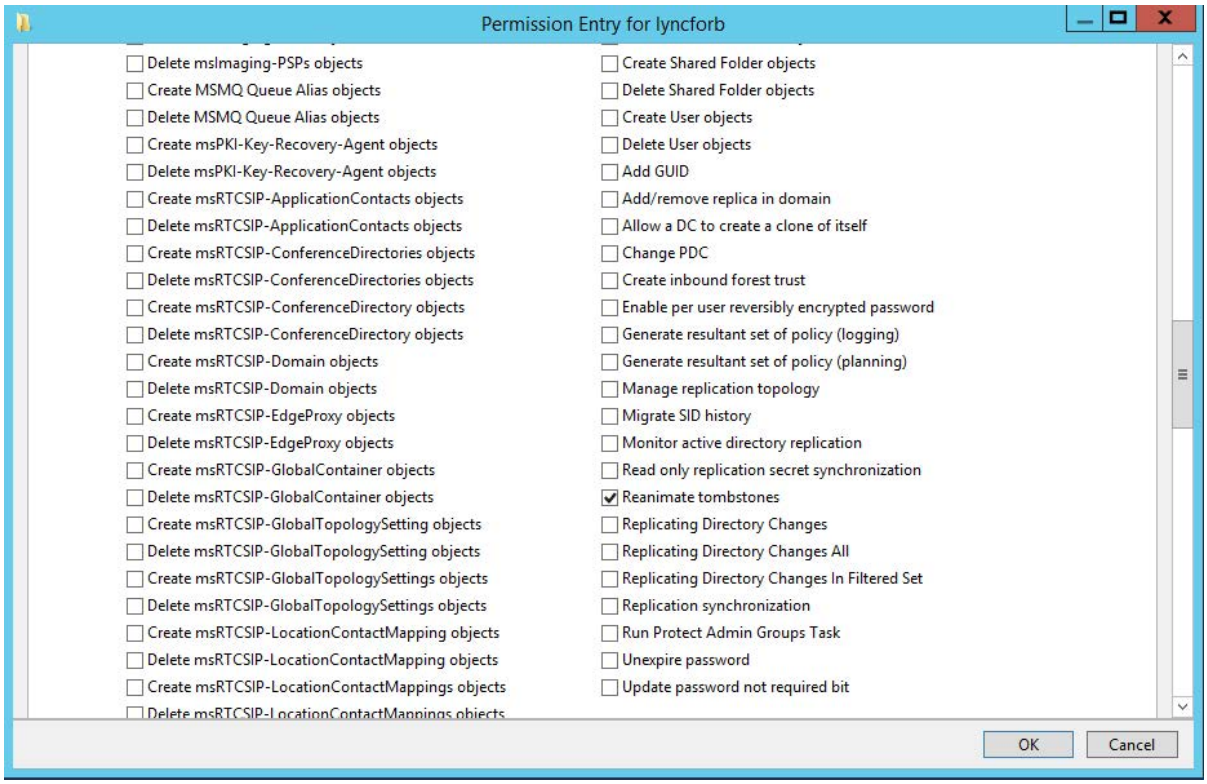


Nota: Sustituya "LukeJohnson" por el principal de seguridad de su elección.

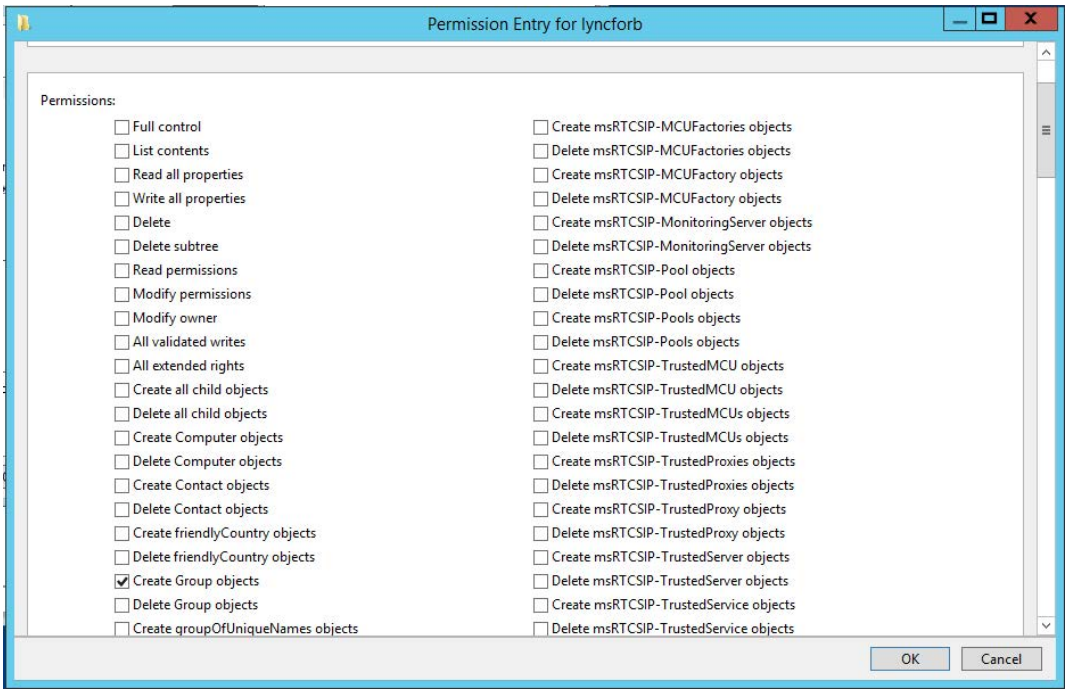
4. A continuación, conéctese al contexto de nomenclatura predeterminado, haga clic derecho en la raíz del dominio y seleccione **Propiedades**.

5. Vaya a la pestaña **Seguridad** y haga clic en **Avanzado**.

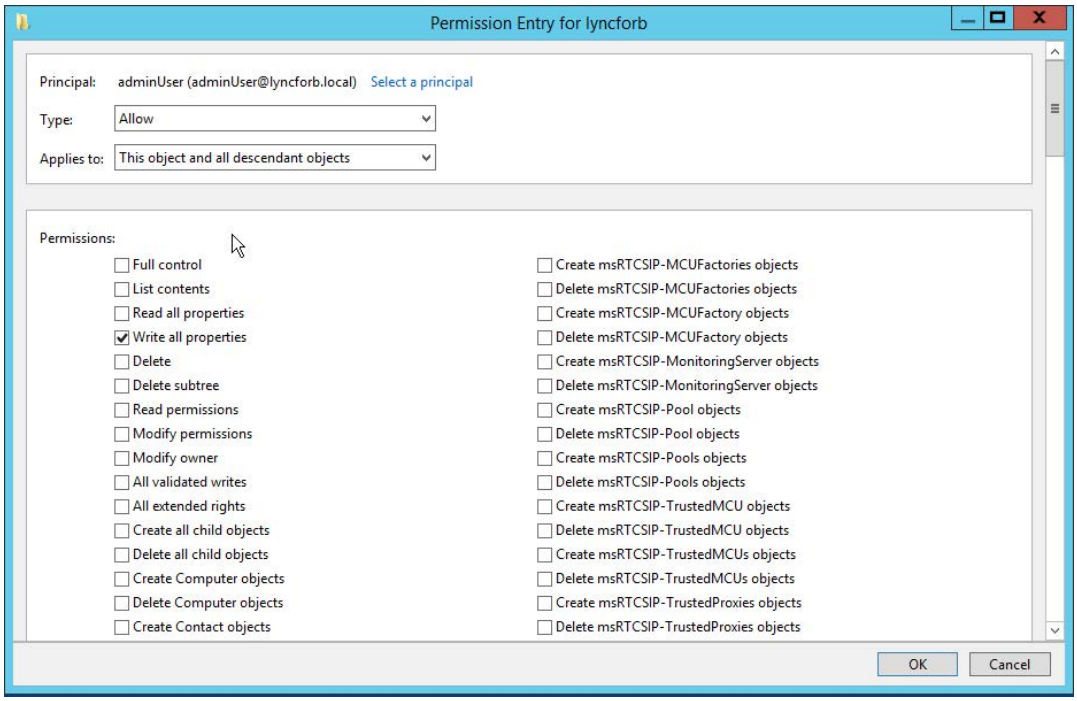
6. Añada el usuario o grupo y seleccione los siguientes derechos:
    a. Reanimate tombstones



b. Crear objetos de grupo



c. Escribir todas las propiedades



Note: Aplique el derecho Reanimate tombstones al objeto que se está protegiendo y a sus objetos descendientes.

7. Haga clic en **Aceptar.**

Nota: Sólo se pueden restaurar los objetos borrados después de delegar los permisos mencionados.

Gestión e informes de GPO

Operación	Permisos necesarios
Crear GPO	- Debe ser miembro del grupo de Propietarios creadores de directivas de grupo
Habilitar/deshabilitar GPO	- Debe tener seleccionado el permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos para Editar ajustes a un grupo o usuario en un GPO, consulte este documento.
Habilitar/deshabilitar los ajustes de configuración del usuario	- Debe tener seleccionado el permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos a un grupo o usuario en un GPO, consulte este documento.
Habilitar/deshabilitar los ajustes de configuración del equipo	- Debe tener seleccionado el permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos a un grupo o usuario en un GPO, consulte este documento.
Habilitar/deshabilitar/eliminar enlaces de GPO	- Debe seleccionar **Vincular GPO** en la lista despegable **Permisos**. **Nota:** Para saber cómo delegar permisos para vincular objetos de directiva de grupo, consulte este documento.
Editar los ajustes de GPO	- Debe tener seleccionado e permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos a un grupo o usuario en un GPO, consulte este documento.
Imponer enlaces GPO	- Debe seleccionar **Vincular GPO** en la lista desplegable **Permisos**. **Nota:** Para saber cómo delegar permisos para vincular objetos de directiva de grupo, consulte este documento.
Informes	- Debe tener el permiso **Leer** en los objetos de Sitio/Dominio/OU (en el atributo gPlink). - Debe tener el permiso **Leer** en los objetos de Sitio/Dominio/OU (en el atributo gPOptions). - Debe tener el permiso **Leer** en los objetos de GPO (en los atributos flags, versionNumber, modifyTimeStamp, createTimeStamp). **Nota:** Por defecto, el grupo Usuarios de dominio tendrá estos derechos para generar informes. Los Administradores de dominio y los Administradores de empresa tendrán todos los derechos mencionados para realizar todas las operaciones de gestión/informes.

Informes de AD

Operaciones	Permisos necesarios
Generar todos los informes de AD	- Debe tener el permiso **Ver** en las OU/dominios deseados.
Generar todos los informes de NTFS	- Debe tener el permiso **Leer** en las carpetas relevantes.

Nota: Además de los permisos mencionados anteriormente, se debe conceder el permiso Replicar cambios de directorio para que la sincronización de datos entre AD y ADManager Plus sea eficaz si la cuenta de servicio no tiene privilegios administrativos de dominio.

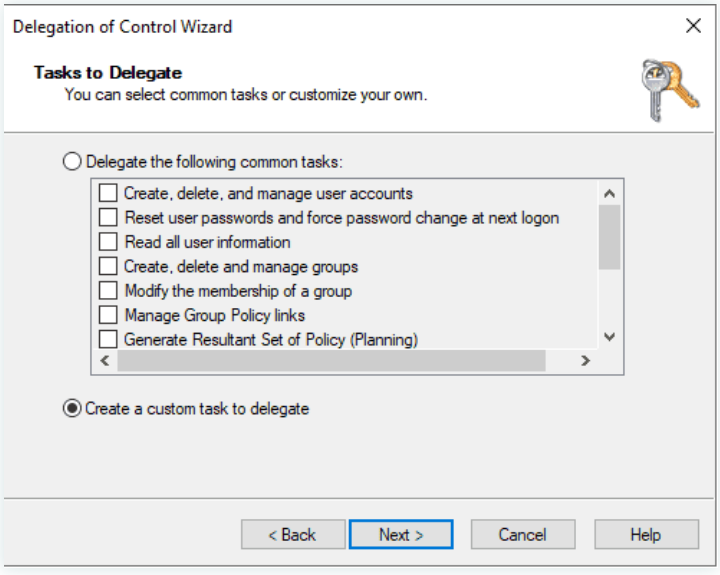
Operación: Generar informes de BitLocker

Permisos necesarios:

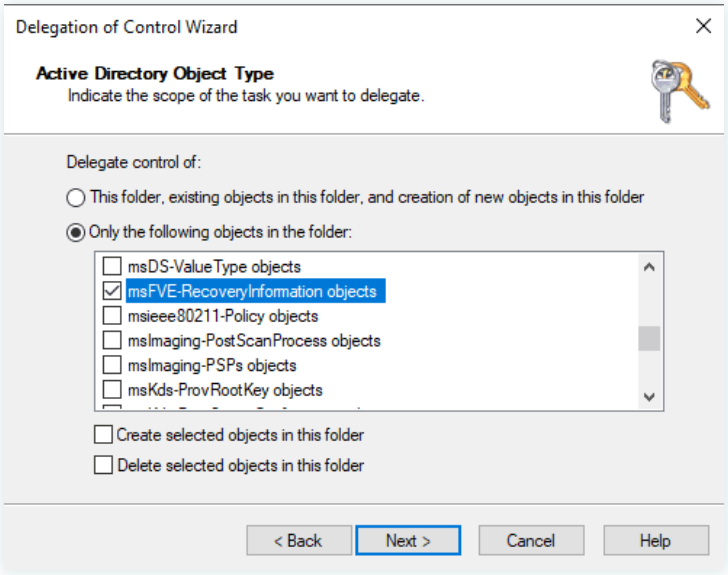
- Debe tener el permiso Ver en las OU y dominios deseados

Pasos para conceder los permisos necesarios para ver las claves de recuperación de BitLocker

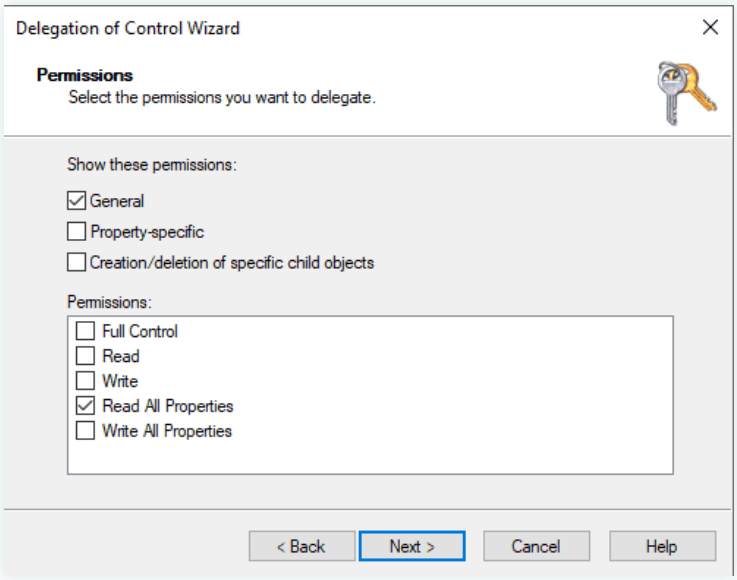
1. Inicie sesión en su controlador de dominio y ejecute **Active Directory Users and Computers**.
2. Localice y haga clic derecho en el **dominio/OU** para el que desea conceder los permisos necesarios y seleccione **Delegar control**. Aparecerá el asistente de Delegación de control.
3. Haga clic en **Siguiente**.
4. Seleccione la cuenta de usuario o grupo deseado y haga clic en **Siguiente**.
5. Seleccione **Crear una tarea personalizada para delegar** y haga clic en **Siguiente**.



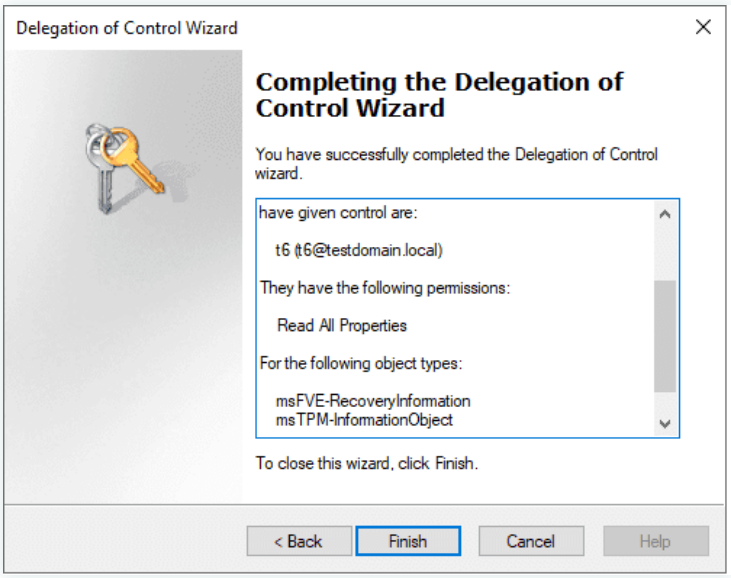
6. Seleccione la opción **Sólo los siguientes objetos en la carpeta**, marque **Objetos msTPM-InformationObject** y **Objetos msFVE-RecoveryInformation**, y luego haga clic en **Siguiente**



7. En la sección **Mostrar estos permisos**, seleccione las opciones **General** y **Específico de la propiedad**.
8. En la sección de permisos, seleccione los permisos **Leer**, **Escribir** y **Leer todas las propiedades** y haga clic en **Siguiente**.



9. Haga clic en **Finalizar.**



Gestión de permisos de archivos

Operaciones	Permisos necesarios
Modificar/eliminar permisos de NTFS	- Debe tener el permiso Leer y Escribir en las carpetas relevantes
Modificar/eliminar permisos de uso compartido	- Se debe poder acceder al recurso compartido desde el equipo en el que está instalado ADManager Plus

Gestión de MS Exchange

Operaciones	Versiones de Exchange	Permisos necesarios
Crear buzones de Exchange mientras se crea la cuenta de usuario correspondiente en AD	Exchange 2007	- Debe tener el rol de Administrador de destinatarios de Exchange y el rol de Operador de cuentas.
	Exchange 2010	- Debe formar parte del grupo de Administración de la organización.
	Exchange 2013	- Debe formar parte del grupo de Administración de la organización.
Crear buzones de Exchange para usuarios existentes de Active Directory	Exchange 2007	- Debe tener el rol de Administrador de destinatarios de Exchange y el rol de Operador de cuentas.
	Exchange 2010	- Debe formar parte del grupo de Administración de la organización.
	Exchange 2013	- Debe formar parte del grupo de Administración de la organización.

Establecer derechos de buzón	Exchange 2007	- Debe tener el rol de administrador de sólo vista de Exchange, permiso de administración del almacén de información y permiso de escritura en el almacén de buzones donde se encuentra el buzón.
	Exchange 2010	- Debe formar parte del grupo de Administración de la organización
	Exchange 2013	- Debe formar parte del grupo de Administración de la organización
Informes de Exchange	Todas las versiones	- Debe tener el rol de Administrador de solo vista de Exchange.

Nota: Sólo los administradores de empresa pueden realizar la gestión de Exchange entre bosques.

Gestión e informes de Microsoft 365

A continuación se enumeran los roles y permisos (alcance mínimo) necesarios para una cuenta de servicio configurada en ADManager Plus.

Módulo	Nombre del rol	Ámbito
Gestión	Administrador de usuarios	Gestionar usuarios, contacts y grupos.
	Administrador de autenticación privilegiado	Restablecer contraseñas y bloquear o desbloquear administradores
	Administrador de roles privilegiados	Gestionar la asignación de roles en Azure Active Directory.
	Administrador de Exchange	Actualizar las propiedades del buzón.
	Administrador del servicio Teams	Gestinar Microsoft Teams.
Informes	Lector global	Obtener informes en todos los servicis de Microsoft 365.
	Lector de seguridad	Obtener acceso de sólo lectura a funciones de seguridad, informes de inicio de sesión y logs de auditoría.

A continuación se enumeran los roles y permisos (alcance mínimo) necesarios para una aplicación de Azure Active Directory configurada en ADManager Plus.

Módulo	Nombre de API	Permiso	Ámbito
Gestión	Gráficos de Microsoft	User.ReadWrite.All	Crear, modificar, eliminar y restaurar usuarios
		Group.ReadWrite.All	Crear, modificar, eliminar y restaurar grupos; agregar o eliminar miembros y propietarios
Informes	Gráficos de Microsoft	User.Read.All	Informes de usuarios y miembros de grupos
		Group.Read.All	Informes de grupos
		Contacts.Read	Informes de contactos
		Reports.Read.All	Informes de uso
		Organization.Read.All	Informes detallados de licencias
		AuditLog.Read.All	Informes de log de auditoría
	Gráficos de Azure Active Directory	Domain.Read.All	Informes basados en dominios

Para conocer los prerrequisitos para configurar una cuenta de Microsoft 365 en ADManager Plus, haga clic aquí.

Migración de Active Directory

Operaciones	Permisos necesarios
Migración de usuario	Administrador de empresa

Gestión e informes de Google Workspace

Operaciones	Permisos necesarios
Gestión	Ámbitos de API: https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.orgunit https://www.googleapis.com/auth/admin.directory.domain.readonly
Informes	Ámbitos de API: https://www.googleapis.com/auth/admin.directory.user

Para conocer los prerrequisitos para configurar una cuenta de G Suite (Google Apps) en ADManager Plus, haga clic aquí.

Prerrequisitos de alta disponibilidad

La alta disponibilidad se refiere a un sistema o componente cuyo objetivo es garantizar el nivel de rendimiento operativo acordado durante un periodo superior al normal. ADManager Plus ayuda a los administradores a mantener la alta disponibilidad de un servidor en caso de fallo del servidor primario.

ADManager Plus lo consigue empleando una arquitectura de alta disponibilidad que designa un servidor de respaldo para que actúe como refuerzo del servidor primario.

- Se utiliza la misma base de datos para los dos servidores y, en un momento dado, uno de ellos atenderá las solicitudes de los usuarios y el otro estará inactivo.
- Cada vez que el servidor primario se encuentra con un tiempo de inactividad imprevisto, el servidor en espera entra en funcionamiento y toma el control de los componentes.

Prerrequisitos:

- Tanto el servidor primario como el secundario deben estar en la misma subred.
- La cuenta de usuario configurada en ambos servicios debe ser miembro del grupo de Administradores de dominio al configurar la alta disponibilidad en ADManager Plus.

Nota:

Más adelante, podrá eliminar esta cuenta de usuario del grupo de Administradores de dominio. Sin embargo, asegúrese de que esta cuenta de usuario tiene los permisos de NTFS y uso compartido tanto en el servidor primario como en el secundario junto con C$ (recurso compartido administrativo).

Si necesita más ayuda o información, escríbanos al correo support@admanagerplus.com o llámenos al +1 844 245 1108.