

NetIQ® eDirectory™ 8.8 SP8

Guía de novedades

Septiembre de 2013



Información legal

ESTE DOCUMENTO Y EL SOFTWARE DESCRITO EN EL MISMO SE FACILITAN DE ACUERDO CON Y SUJETOS A LOS TÉRMINOS DE UN ACUERDO DE LICENCIA O DE UN ACUERDO DE NO DIVULGACIÓN. EXCEPTO EN LA FORMA ESTABLECIDA EXPRESAMENTE EN EL MENCIONADO ACUERDO DE LICENCIA O ACUERDO DE NO DIVULGACIÓN, NETIQ CORPORATION PROPORCIONA ESTE DOCUMENTO Y EL SOFTWARE DESCRITO EN EL MISMO "TAL COMO ESTÁN" SIN NINGÚN TIPO DE GARANTÍA, YA SEA EXPRESA O IMPLÍCITA, INCLUIDA SIN LIMITACIÓN, CUALQUIER GARANTÍA EXPRESA DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN EN PARTICULAR. ALGUNOS ESTADOS O JURISDICCIONES NO PERMITEN LAS EXENCIONES DE GARANTÍA EXPRESAS O IMPLÍCITAS EN DETERMINADAS TRANSACCIONES; POR TANTO, ESTE ENUNCIADO PODRÍA NO SER DE APLICACIÓN EN SU CASO.

A efectos de claridad, cualquier módulo, adaptador u otro material similar ("Módulo") se concede bajo licencia de acuerdo con los términos y condiciones del Acuerdo de licencia del usuario final correspondiente a la versión aplicable del producto o software de NetIQ con el que se relaciona o interactúa y, al acceder al Módulo, copiarlo o usarlo, usted se compromete a quedar vinculado por dichos términos. Si no está de acuerdo con los términos del Acuerdo de licencia del usuario final, entonces no está autorizado para usar, acceder a o copiar el Módulo, y deberá destruir todas las copias del Módulo y ponerse en contacto con NetIQ para recibir más instrucciones.

Se prohíbe prestar, vender, alquilar o entregar este documento y el software descrito en este documento de ninguna forma sin el permiso previo por escrito de NetIQ Corporation, excepto en la medida permitida por la ley. Excepto según se establece en el mencionado acuerdo de licencia o acuerdo de no divulgación, se prohíbe la reproducción, almacenamiento en un sistema de recuperación o transmisión por cualquier medio, ya sea electrónico, mecánico o de otro tipo, de cualquier parte de este documento o del software descrito en este documento sin el permiso previo por escrito de NetIQ Corporation. Algunas empresas, nombres y datos mencionados en este documento se utilizan con fines ilustrativos y puede que no representen a empresas, personas o datos reales.

Este documento podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información contenida en este documento. Estos cambios pueden incorporarse en nuevas ediciones de este documento. NetIQ Corporation puede realizar mejoras o cambios en el software descrito en este documento en cualquier momento.

Derechos restringidos del Gobierno de los Estados Unidos: si el software y la documentación se adquieren por parte de o en nombre del gobierno de los Estados Unidos o por parte de un contratista o subcontratista (en cualquier nivel) principal del gobierno de los Estados Unidos, de conformidad con 48 C.F.R. 227.7202-4 (para adquisiciones del Departamento de Defensa [DOD]) y con 48 C.F.R. 2.101 y 12.212 (para adquisiciones que no sean del DOD), los derechos del gobierno sobre el software y la documentación, incluidos los derechos de uso, modificación, reproducción, publicación, actuación, visualización o divulgación estarán sujetos en todas sus vertientes a los derechos y restricciones de licencia comercial establecidos en el presente acuerdo de licencia.

© 2013 NetIQ Corporation y sus afiliados. Reservados todos los derechos.

Para obtener información acerca de las marcas comerciales de NetIQ, consulte <https://www.netiq.com/company/legal/>.

Tabla de contenido

Acerca de este libro y la biblioteca	7
Acerca de NetIQ Corporation	9
1 Funciones y mejoras del Service Pack 8	11
1.1 Mejoras de escalabilidad	11
1.1.1 Control de procesos en segundo plano	11
1.1.2 Proceso skulker	11
1.1.3 Replicación asincrónica	12
1.1.4 Replicación basada en directiva	12
1.1.5 Obituario	12
1.1.6 Seguimiento del número de obituarios y del número de objetos en el caché de cambios a través de iMonitor	12
1.1.7 Enlaces de referencia distribuidos (DRL)	12
1.1.8 Almacenamiento en caché de eventos del diario	13
1.1.9 Compatibilidad con discos de estado sólido (SSD)	13
1.1.10 Coste de referencia avanzado (ARC)	13
1.1.11 Intervalo de actualización de entrada	13
1.2 Mejoras de LDAP	13
1.2.1 Control de modificación permisivo	14
1.2.2 Compatibilidad de hora generalizada	14
1.2.3 Control de supresión de subárbol	14
1.3 compatibilidad con IPv6	14
1.4 Mejoras de auditoría	15
2 Plataformas admitidas para la instalación de eDirectory	17
2.1 Plataformas obsoletas	17
2.2 Linux	17
2.3 Windows	18
3 Mejoras de instalación y actualización	19
3.1 Varios formatos de paquete para instalar eDirectory 8.8	20
3.2 Instalación de eDirectory 8.8 en una ubicación personalizada	20
3.2.1 Especificación de una ubicación personalizada para los archivos de aplicación	20
3.2.2 Especificación de una ubicación por defecto para los archivos de datos	21
3.2.3 Especificación de una ubicación predeterminada para los archivos de configuración	21
3.3 Instalación por un usuario diferente de root	22
3.4 Compatibilidad mejorar para instalaciones en clústeres de alta disponibilidad	22
3.5 Cumplimiento de estándares	22
3.5.1 Conformidad con FHS	23
3.5.2 Conformidad con LSB	24
3.6 Comprobaciones de actividad del servidor	24
3.6.1 Necesidad de ejecutar comprobaciones de actividad	24
3.6.2 ¿Qué hace que un servidor tenga una actividad congruente?	24
3.6.3 Realización de comprobaciones de la actividad	24
3.6.4 Tipos de comprobaciones de actividad	25
3.6.5 Categorización de la actividad	26
3.6.6 Archivos de registro	27
3.7 Integración de SecretStore con eDirectory	28

3.8	Instalación de Utilidades de eDirectory	28
3.9	Información adicional	28
4	Copia de seguridad y recuperación de NICI	31
5	La utilidad ndspassstore	33
6	Múltiples instancias	35
6.1	Necesidad de múltiples instancias	35
6.2	Ejemplos de escenarios de implementación de múltiples instancias	35
6.3	Uso de múltiples instancias	36
6.3.1	Planificación de la instalación	36
6.3.2	Configuración de múltiples instancias	36
6.4	Gestión de múltiples instancias	37
6.4.1	La utilidad ndsmanage	37
6.4.2	Identificación de una instancia específica	41
6.4.3	Invocar una utilidad para una instancia específica	41
6.5	Ejemplo de escenario de múltiples instancias	41
6.5.1	Planificación de la instalación	41
6.5.2	Configuración de las instancias	42
6.5.3	Invocar una utilidad para una instancia	42
6.5.4	Listado de las instancias configuradas	42
6.6	Información adicional	42
7	Autenticación en eDirectory a través de SASL GSSAPI	43
7.1	Conceptos	43
7.1.1	¿Qué es Kerberos?	43
7.1.2	¿Qué es SASL?	44
7.1.3	¿Qué es GSSAPI?	44
7.2	¿Cómo funciona GSSAPI con eDirectory?	44
7.3	Configuración de GSSAPI	45
7.4	¿Cómo utiliza LDAP GSSAPI?	45
7.5	Términos comunes	46
8	Aplicación de contraseñas universales que diferencian mayúsculas de minúsculas	47
8.1	Necesidad de contraseñas que distinguen mayúsculas de minúsculas	47
8.2	Cómo hacer que la contraseña distinga mayúsculas de minúsculas	48
8.2.1	Requisitos previos	48
8.2.2	Cómo hacer que la contraseña distinga mayúsculas de minúsculas	48
8.2.3	Gestión de contraseñas que distinguen entre mayúsculas y minúsculas	49
8.3	Actualización de las utilidades y los clientes heredados de Novell	49
8.3.1	Migración a contraseñas que distinguen entre mayúsculas y minúsculas	50
8.4	Cómo impedir que los clientes heredados de Novell accedan al servidor de eDirectory 8.8.	50
8.4.1	Necesidad de evitar que los clientes heredados de Novell accedan al servidor de eDirectory 8.8	51
8.4.2	Gestión de las configuraciones de entrada de NDS	51
8.4.3	Operaciones de partición	55
8.4.4	Aplicación de contraseñas que distinguen mayúsculas de minúsculas en un árbol mixto	55
8.5	Información adicional	55

9	Compatibilidad con la directiva de contraseñas de Microsoft Windows Server 2008	57
9.1	Creación de directivas de contraseñas de Windows Server 2008	57
9.2	Gestión de directivas de contraseñas de Windows Server 2008	58
9.3	Información adicional	58
10	Sincronización de prioridad	59
10.1	Necesidad de sincronización de prioridad	59
10.2	Uso de sincronización de prioridad	60
10.3	Información adicional	60
11	Cifrado de datos	61
11.1	Atributos de cifrado	61
11.1.1	Necesidad de atributos cifrados	61
11.1.2	Cómo cifrar los atributos	62
11.1.3	Acceda a los atributos cifrados	62
11.2	Cifrado de replicación	62
11.2.1	Necesidad de réplica cifrada	62
11.2.2	Cómo habilitar la réplica cifrada	63
11.3	Información adicional	63
12	Rendimiento de carga general	65
13	Módulos auxiliares (plug-in) ICE de iManager	67
13.1	Agregar esquema que falta	67
13.1.1	Agregar el esquema desde un archivo	67
13.1.2	Agregar el esquema desde un servidor	68
13.2	Comparar el esquema	69
13.2.1	Comparar archivos de esquema	69
13.2.2	Comparar esquema entre un servidor y un archivo	69
13.3	Generar un archivo de orden	69
13.4	Información adicional	69
14	Copia de seguridad basada en LDAP	71
14.1	Necesidad de copia de seguridad basada en LDAP	71
14.2	Información adicional	72
15	Obtener lista de privilegios eficaces de LDAP	73
15.1	Necesidad de interfaz para obtener lista de privilegios eficaces de LDAP	73
15.2	Información adicional	73
16	Gestión del registro de errores en eDirectory 8.8	75
16.1	Niveles de gravedad del mensaje	75
16.1.1	Fatal	75
16.1.2	Advertencia	75
16.1.3	Error	76
16.1.4	Información	76
16.1.5	Depurar	76
16.2	Configuración del registro de errores	76

16.2.1	Linux	77
16.2.2	Windows	77
16.3	Mensajes de DStTrace	79
16.3.1	Linux	79
16.3.2	Windows	80
16.4	Filtrado de mensajes de iMonitor	82
16.5	Filtrado de mensajes de SAL	82
16.5.1	Configuración de los niveles de gravedad	82
16.5.2	Definición de la vía al archivo de registro	83
17	Utilidad de carga general sin conexión: Idif2dib	85
17.1	Necesidad de Idif2dib	85
17.2	Información adicional	85
18	Copia de seguridad de eDirectory con SMS	87
19	Auditoría de LDAP	89
19.1	Necesidad de auditoría de LDAP	89
19.2	Uso de auditoría LDAP	89
19.3	Información adicional	90
20	Auditoría con XDASv2	91
21	Miscelánea	93
21.1	Generación de informes sobre volcado de caché en iMonitor	93
21.2	Compatibilidad de sintaxis de entero grande de Microsoft en iManager	93
21.3	Almacenamiento en caché del objeto de seguridad	94
21.4	Mejora del rendimiento de la búsqueda de subárbol	94
21.5	Cambios de localhost	95
21.6	Controlador de archivo 256 en Solaris	95
21.7	Administrador de memoria en Solaris	95
21.8	Grupos anidados	95

Acerca de este libro y la biblioteca

La *Guía de novedades* le presenta las nuevas funciones de NetIQ eDirectory.

Para conocer la versión más reciente de la *Guía de novedades de NetIQ eDirectory 8.8 SP8*, consulte el sitio web de [documentación en línea de NetIQ eDirectory 8.8](#).

A quién va dirigida

Esta guía está dirigida a administradores de red.

Otra información de la biblioteca

La biblioteca ofrece los siguientes recursos informativos:

Guía de administración de XDASv2

Describe cómo configurar y usar XDASv2 para auditar eDirectory y NetIQ Identity Manager.

Guía de instalación

Describe cómo instalar eDirectory. Está dirigida a los administradores de red.

Guía de administración

Describe cómo gestionar y configurar eDirectory.

Guía de resolución de problemas

Describe cómo solucionar problemas en eDirectory.

Guía de ajuste para plataformas Linux

Describe cómo analizar y ajustar eDirectory en las plataformas Linux para producir un rendimiento superior en todas las implementaciones.

Estas guías están disponibles en el [sitio web de documentación de NetIQ eDirectory 8.8 \(https://www.netiq.com/documentation/edir88/\)](https://www.netiq.com/documentation/edir88/).

Para obtener información sobre la utilidad de gestión de eDirectory, consulte la *NetIQ iManager 2.7 Administration Guide* (<https://www.netiq.com/documentation/imanager/>) (Guía de administración de NetIQ iManager 2.7).

Acerca de NetIQ Corporation

Somos una empresa mundial de software empresarial, centrada en resolver los tres principales desafíos de su entorno, a saber, cambios, complejidad y riesgo, y en cómo podemos ayudarle a controlarlos.

Nuestro punto de vista

La adaptación a los cambios y la gestión de la complejidad y los riesgos no son conceptos nuevos

De hecho, de todos los desafíos a los que se enfrenta, quizá sean estas las variables más destacadas que le deniegan el control necesario para poder medir, supervisar y gestionar de forma segura sus entornos físico, virtual y de cloud computing.

Activación de servicios esenciales para el negocio de forma más rápida y eficiente

Creemos que la única forma de hacer posible una prestación de servicios más puntual y económica es dotar a las organizaciones de TI del mayor control posible. La presión continua de los cambios y la complejidad seguirá aumentando a medida que las organizaciones sigan creciendo y las tecnologías necesarias para gestionarlas se hagan intrínsecamente más complejas.

Nuestra filosofía

Vender soluciones inteligentes, no solo software

Para poder ofrecer un control fiable, debemos entender primero los escenarios reales en los que —día a día— operan las organizaciones de TI como la suya. Esa es la única forma de desarrollar soluciones de TI prácticas e inteligentes que proporcionen resultados conmensurables con una eficacia demostrada. Y eso es mucho más satisfactorio que vender simplemente software.

Fomentar su éxito es nuestra pasión

Ayudarle a alcanzar el éxito es el objetivo primordial de nuestro trabajo. Desde la concepción al desarrollo, sabemos que usted necesita soluciones de TI que funcionen bien y se integren a la perfección con su inversión existente; necesita asistencia continua y formación posterior a la implementación; y, para variar, también necesita trabajar con alguien que le facilite las cosas. En definitiva, su éxito será también el nuestro.

Nuestras soluciones

- ♦ Control de identidad y acceso
- ♦ Gestión de acceso
- ♦ Gestión de la seguridad
- ♦ Gestión de sistemas y aplicaciones
- ♦ Gestión del trabajo
- ♦ Gestión de servicios

Cómo contactar con asistencia para ventas

Para cualquier pregunta sobre nuestros productos, precios y capacidades, póngase en contacto con su representante local. Si no puede contactar con su representante local, comuníquese con nuestro equipo de Asistencia para ventas.

Oficinas mundiales:	www.netiq.com/about_netiq/officelocations.asp
Estados Unidos y Canadá:	1-888-323-6768
Correo electrónico:	info@netiq.com
sitio Web de iFolder:	www.netiq.com

Cómo ponerse en contacto con el personal de asistencia técnica

Para obtener información sobre problemas con productos específicos, póngase en contacto con nuestro equipo de asistencia técnica.

Oficinas mundiales:	www.netiq.com/support/contactinfo.asp
Norteamérica y Sudamérica:	1-713-418-5555
Europa, Oriente Medio y África:	+353 (0) 91-782 677
Correo electrónico:	support@netiq.com
sitio Web de iFolder:	www.netiq.com/support

Cómo contactar con asistencia para documentación

Nuestro objetivo es proporcionar documentación que satisfaga sus necesidades. Si tiene sugerencias de mejoras, haga clic en **Add Comment** (Agregar comentario) en la parte de abajo de cualquier página de las versiones HTML de la documentación publicada en www.netiq.com/documentation. Si lo desea, también puede enviar un correo electrónico a Documentation-Feedback@netiq.com. Agradecemos sus comentarios y estamos deseando oír sus sugerencias.

Cómo contactar con la Comunidad de usuarios en línea

Qmunity, la comunidad de NetIQ en línea, es una red de colaboración que le pone en contacto con sus colegas y con otros expertos de NetIQ. Qmunity le ayuda a dominar los conocimientos que necesita para hacer realidad todo el potencial de su inversión en TI de la que depende, al proporcionarle información inmediata, enlaces útiles a recursos prácticos y acceso a los expertos de NetIQ. Para obtener más información, visite la página <http://community.netiq.com>.

1 Funciones y mejoras del Service Pack 8

En este capítulo se presenta una descripción general de las funciones y mejoras incluidas en eDirectory 8.8 SP8.

1.1 Mejoras de escalabilidad

A fin de garantizar una sincronización de datos y un procesamiento de obituario más rápidos y de reducir el uso de memoria al procesar eventos del registro, en eDirectory 8.8 SP8 se incluyen las mejoras de escalabilidad descritas en las secciones siguientes.

En esta versión, se han modificado ciertos procesos que se realizan en segundo plano a fin de satisfacer las necesidades de entornos dinámicos más grandes. Esto incluye la optimización de los procesos en segundo plano existentes y proporcionar opciones de configuración para ajustar los sistemas para que se adapten mejor a su entorno.

1.1.1 Control de procesos en segundo plano

Los administradores pueden controlar el proceso en segundo plano al configurar las siguientes directivas de Ajustes de retraso del proceso en segundo plano en la ventana correspondiente de NetIQ iMonitor:

- ♦ **CPU:** especifica el porcentaje máximo de recursos informáticos y la duración máxima del estado de reposo del mismo proceso (skulker, depurador u obituario).
- ♦ **Límite rígido:** especifica un ajuste de retraso estático para los procesos individuales skulker, depurador y obituario.

Para obtener información acerca de la configuración de los procesos en segundo plano, consulte [“Configuring Background Processes”](#) (Configuración de los procesos en segundo plano) de la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.1.2 Proceso skulker

Con el fin de aumentar los hilos creados para replicar en más servidores de manera simultánea, puede usar el proceso skulker para establecer manualmente el número máximo de hilos creados. Este ajuste se aplica a todas las particiones de un servidor.

Para obtener información sobre el proceso skulker, consulte [“Manually Configuring Synchronization Threads”](#) (Configuración manual de hilos de sincronización) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.1.3 Replicación asincrónica

A fin de disminuir la cantidad de tiempo que requiere la replicación, se ejecutan en paralelo las siguientes operaciones:

- ♦ Procesamiento del caché de cambios
- ♦ Envío de paquetes a un servidor remoto

La nueva opción **Ajustes de sincronización saliente asincrónica (milésimas de segundo)** permite evitar la sobrecarga del servidor receptor. Esta opción está inhabilitada por defecto. El ajuste depende del entorno. Cuando habilite esta opción, configúrela en 100 y luego aumente o reduzca el valor según sea necesario.

Para obtener información acerca de la sincronización saliente asincrónica, consulte [“Configuring Asynchronous Outbound Synchronization”](#) (Configuración de sincronización saliente asincrónica) de *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.1.4 Replicación basada en directiva

Ahora los administradores pueden crear una directiva (archivo XML) para especificar cómo replicar cambios. Por ejemplo, esto puede resultar útil con un anillo de réplicas distribuido entre múltiples ubicaciones. Si la directiva incluye un error tipográfico o una sintaxis incorrecta, la replicación revierte al método por defecto.

Para obtener más información, consulte [“Policy Based Replication”](#) (Replicación basada en directivas) de la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.1.5 Obituario

Un obituario se genera cuando las operaciones de suprimir, cambiar de nombre o mover un objeto se procesan más rápidamente que en versiones anteriores de eDirectory. Por ejemplo, una actualización que requería cinco ciclos en las versiones anteriores ahora podría necesitar solo dos ciclos.

Además, el proceso de obituario ahora puede ejecutarse en paralelo con el proceso skulker.

1.1.6 Seguimiento del número de obituarios y del número de objetos en el caché de cambios a través de iMonitor.

iMonitor muestra el número de objetos con los obituarios de cada estado. Asimismo, muestra el número de objetos en el caché de cambios de una partición cuando se visualiza un objeto de partición a través de iMonitor en un servidor determinado. Esto ayuda a supervisar mejor el estado de la sincronización y el procesamiento obituarios.

1.1.7 Enlaces de referencia distribuidos (DRL)

Para optimizar el procesamiento de obituarios, eDirectory ya no utiliza los siguientes atributos de DLR:

- ♦ Usado por
- ♦ Obituario usado por

1.1.8 Almacenamiento en caché de eventos del diario

El sistema de eventos del diario se modifica para permitirle usar una combinación de memoria y disco para mantener los eventos en la cola. De esta forma se reduce de forma drástica el aumento de memoria en el proceso ndsd.

Entre las mejoras en los eventos del diario se incluyen:

- ♦ **Almacenamiento en el caché**

Cuando la cola de eventos del diario aumenta por encima de un punto de memoria (32 MB = máx. de 8 bloques x 4 MB), eDirectory comienza a usar el caché en la unidad de disco duro.

- ♦ **Variables**

Los eventos del diario incluyen las siguientes variables que los usuarios pueden configurar:

- ♦ NDS_EVENT_DISK_CACHE
- ♦ NDS_EVENT_DISK_CACHE_DIR

- ♦ **Compresión**

Una compresión mejorada reduce al mínimo el tamaño de los datos en el disco duro. El índice de compresión es de aproximadamente 20:1.

1.1.9 Compatibilidad con discos de estado sólido (SSD)

Esta versión es compatible con Enterprise SSD para mejorar las operaciones de E/S.

1.1.10 Coste de referencia avanzado (ARC)

En esta versión, ARC está habilitado por defecto.

Para obtener más información, consulte "[Advanced Referral Costing](#)" (Coste de referencia avanzado) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.1.11 Intervalo de actualización de entrada

La nueva opción Intervalo de inhabilitación de la actualización de entrada permite a los administradores especificar un intervalo de tiempo (en segundos) durante el que eDirectory no actualiza los atributos de entrada.

Nota: Esta opción se aplica solamente a las entradas de Servicios de directorio de (NDS).

Para obtener más información, consulte "[Controlling and Configuring the DS Agent](#)" (Control y configuración de Agente DS) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.2 Mejoras de LDAP

Esta versión incluye las siguientes mejoras de LDAP:

1.2.1 Control de modificación permisivo

Puede ampliar la operación de modificación de LDAP actual mediante esta opción. Si trata de suprimir un atributo que no existe o añadir un cualquier valor a un atributo existente, la operación se produce sin mostrar ningún mensaje de error.

Para obtener más información, consulte [“Configuring Permissive Modify Control”](#) (Configuración del control de modificación permisivo) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.2.2 Compatibilidad de hora generalizada

La opción de compatibilidad de hora generalizada permite mostrar la hora en el formato AAAAMMDDHHmmSS.0Z.

Tenga en cuenta que 0Z indica compatibilidad con fracciones de segundo tal como se admite en Active Directory. Puesto que eDirectory no es compatible con la visualización de fracciones de segundo, esta opción muestra 0 para evitar romper esa funcionalidad en un entorno coexistente.

Para obtener más información, consulte [“Configuring Generalized Time Support”](#) (Configuración de compatibilidad de hora generalizada) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

1.2.3 Control de supresión de subárbol

Esta versión admite el control de supresión de subárbol que permite suprimir cualquier objeto de contenedor. Anteriormente, solo podían suprimirse los objetos hojas. No obstante, el control de supresión de subárbol no admite la supresión de contenedores de partición.

1.3 compatibilidad con IPv6

Esta versión es compatible tanto con IPv4 como con IPv6. IPv6 está habilitado automáticamente por defecto al instalar eDirectory. Si va a actualizar desde una versión anterior de eDirectory, debe habilitar automáticamente la compatibilidad con IPv6.

eDirectory 8.8 SP8 admite los siguientes modos de IPv6:

- ♦ Pila doble
- ♦ Proceso de túnel
- ♦ IPv6 puro

eDirectory 8.8 SP8 no admite los siguientes tipos de dirección de IPv6:

- ♦ Direcciones locales de enlace
- ♦ Direcciones IPv6 asignadas con IPv4
- ♦ Direcciones IPv6 compatibles con IPv4

eDirectory 8.8 SP8 admite los siguientes formatos de direcciones:

- ♦ [::]
- ♦ [::1]
- ♦ [2015::12]
- ♦ [2015::12]:524

1.4 Mejoras de auditoría

Esta versión mejora la auditoría de XDAS al admitir la dirección IP de cliente en eventos.

2 Plataformas admitidas para la instalación de eDirectory

eDirectory 8.8 SP8 es una versión compatible entre diversas plataformas dirigida a mejorar la estabilidad de eDirectory.

2.1 Plataformas obsoletas

eDirectory 8.8 SP8 no es compatible con las plataformas siguientes:

- ♦ NetWare
- ♦ eDirectory de 32 bits y 64 bits en Solaris
- ♦ eDirectory de 32 bits en AIX
- ♦ eDirectory de 32 bits en Linux
- ♦ eDirectory de 32 bits en Windows

2.2 Linux

Debe instalar eDirectory en una de las siguientes plataformas:

- ♦ SLES 11 SP1, SP2 y SP3 de 64 bits
- ♦ SLES 10 SP4 64 bits
- ♦ RHEL 5.7, 5.8 y 5.9
- ♦ RHEL 6.2, 6.3 y 6.4

Estos sistemas operativos se pueden ejecutar en modo virtual en los siguientes hipervisores:

- ♦ VMware ESXi
- ♦ Xen (en SLES 10 y SLES 11 y sus paquetes de soporte)

Nota: eDirectory 8.8 SP8 es compatible con el servicio de virtualización de SLES 10 XEN que se ejecuta en el SO guest de SLES 10. En el [sitio web de actualización de NetIQ \(https://update.novell.com\)](https://update.novell.com) están disponibles las siguientes actualizaciones:

- ♦ SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
- ♦ SLES10-Updates

Para registrar y actualizar SUSE Linux Enterprise 10, consulte [Registering SUSE Linux Enterprise with the NetIQ Customer Center \(http://www.suse.com/products/register.html\)](http://www.suse.com/products/register.html) (Registro de SUSE Linux Enterprise en el Centro de servicios al cliente de NetIQ). Después de instalar la actualización más reciente, asegúrese de que el nivel de parche mínimo de la actualización instalada sea 3.0.2_09763-0.8.

- ♦ Virtualización de Windows Server 2008 R2 con Hyper-V

Para determinar la versión de SUSE Linux que está ejecutando, consulte el archivo `/etc./SuSE-release`.

Asegúrese de que se aplican las revisiones de glibc más recientes de [Red Hat Errata \(http://rhn.redhat.com/errata\)](http://rhn.redhat.com/errata) en sistemas Red Hat. La versión mínima requerida de la biblioteca glibc es la 2.1.

2.3 Windows

Debe instalar eDirectory en una de las siguientes plataformas:

- ♦ Windows Server 2008 (x64) (Standard/Enterprise/Data Center Edition) y sus paquetes de servicio
- ♦ Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition) y sus paquetes de servicio
- ♦ Servidor Windows 2012

Importante

- ♦ Debe utilizar una cuenta que tenga derechos administrativos para instalar eDirectory 8.8 SP8 en un Windows Server 2008 R2.
 - ♦ No se admiten las versiones de escritorio Windows.
-

3 Mejoras de instalación y actualización

En este capítulo se analizan las nuevas funciones y mejoras de la instalación y actualización de NetIQ eDirectory 8.8.

En la siguiente tabla se enumeran las nuevas funciones y se especifican las plataformas que las admiten.

Función	Linux	Windows
Varios formatos de paquete para instalar eDirectory 8.8	✓	✗
Instalación de ubicación personalizada para archivos de aplicación	✓	✓
Instalación de ubicación personalizada para archivos de datos	✓	✓
Instalación de ubicación personalizada para archivos de configuración	✓	✗
Instalación por un usuario diferente de root	✓	✗
Soporte mejorado para las instalaciones en clústeres de alta disponibilidad	✓	✓
Conformidad con FHS	✓	✗
Conformidad con LSB	✓	✗
Comprobaciones de la actividad del servidor	✓	✓
Integración de SecretStore	✓	✓
Instalación de Utilidades de eDirectory	✓	✓

En este capítulo se proporciona la siguiente información:

- ♦ Sección 3.1, “Varios formatos de paquete para instalar eDirectory 8.8”, en la página 20
- ♦ Sección 3.2, “Instalación de eDirectory 8.8 en una ubicación personalizada”, en la página 20
- ♦ Sección 3.3, “Instalación por un usuario diferente de root”, en la página 22
- ♦ Sección 3.4, “Compatibilidad mejorar para instalaciones en clústeres de alta disponibilidad”, en la página 22
- ♦ Sección 3.5, “Cumplimiento de estándares”, en la página 22
- ♦ Sección 3.6, “Comprobaciones de actividad del servidor”, en la página 24
- ♦ Sección 3.7, “Integración de SecretStore con eDirectory”, en la página 28
- ♦ Sección 3.8, “Instalación de Utilidades de eDirectory”, en la página 28
- ♦ Sección 3.9, “Información adicional”, en la página 28

3.1 Varios formatos de paquete para instalar eDirectory 8.8

En Linux, existe la opción de elegir entre diversos formatos de archivo al instalar eDirectory 8.8 en el host. Los formatos de archivo se muestran en la siguiente tabla.

Tipo de usuario y ubicación de instalación	Linux
Usuario root	
Ubicación por defecto	RPM
Ubicación personalizada	Archivo tar
Usuario diferente de root	
Ubicación personalizada	Archivo tar

Para obtener más información sobre la instalación de archivos tar, consulte la [NetIQ eDirectory 8.8 SP8 Installation Guide](#) (Guía de instalación de NetIQ eDirectory 8.8 SP8).

3.2 Instalación de eDirectory 8.8 en una ubicación personalizada

eDirectory 8.8 le ofrece la flexibilidad de instalar la aplicación, los archivos de datos y los archivos de configuración en la ubicación que usted elija.

Un escenario de instalación de eDirectory 8.8 en una ubicación personalizada se produce cuando ya tiene instalada una versión anterior de eDirectory y desea probar eDirectory 8.8 antes de actualizar a esta versión. De esta forma, puede dejar intacta la instalación actual de eDirectory mientras prueba la nueva versión. Puede decidir si desea conservar la versión existente o actualizar a eDirectory 8.8.

Nota: SLP y el subagente SNMP se instalan en las ubicaciones por defecto.

En esta sección se explica cómo instalar los diversos archivos en una ubicación personalizada:

- ♦ [Sección 3.2.1, “Especificación de una ubicación personalizada para los archivos de aplicación”, en la página 20](#)
- ♦ [Sección 3.2.2, “Especificación de una ubicación por defecto para los archivos de datos”, en la página 21](#)
- ♦ [Sección 3.2.3, “Especificación de una ubicación predeterminada para los archivos de configuración”, en la página 21](#)

3.2.1 Especificación de una ubicación personalizada para los archivos de aplicación

Mientras instala eDirectory, puede instalar los archivos de aplicación en una ubicación que usted elija.

Linux

Para instalar eDirectory 8.8 en una ubicación personalizada, puede usar el archivo de instalación tar y desempaquetar eDirectory 8.8 en la ubicación elegida.

Windows

Ya se podía especificar una ubicación personalizada para los archivos de aplicación en el asistente de instalación incluso antes de eDirectory 8.8.

3.2.2 Especificación de una ubicación por defecto para los archivos de datos

Al configurar eDirectory, puede guardar los archivos de datos en la ubicación que usted elija. Entre los archivos de datos se incluyen los directorios `data`, `dib` y `log`.

Linux

Para configurar los archivos de datos en una ubicación personalizada, puede usar la opción `-d` o `-D` de la utilidad `ndsconfig`.

Opción	Descripción
<code>-d custom_location</code>	Crea el directorio <code>DIB</code> (la base de datos de eDirectory) en la vía mencionada. Nota: Esta opción estaba presente también antes de eDirectory 8.8.
<code>-D custom_location</code>	Crea los directorios <code>data</code> (contiene datos como pids e IDs de zócalo), <code>dib</code> y <code>log</code> en la vía mencionada.

Windows

En Windows se indicará que es necesario introducir la vía a `DIB` durante la instalación. Introduzca la vía deseada.

3.2.3 Especificación de una ubicación predeterminada para los archivos de configuración

Al configurar eDirectory, puede seleccionar la vía en la que desea configurar sus archivos de configuración.

Linux

Para configurar el archivo de configuración `nds.conf` en otra ubicación, utilice la opción `--config-file` de la utilidad `ndsconfig`.

Para instalar los demás archivos de configuración (como `modules.conf`, `ndsimon.conf` y `ice.conf`) en otra ubicación, realice lo siguiente:

- 1 Copie todos los archivos de configuración en la nueva ubicación.
- 2 Defina la nueva ubicación introduciendo los siguientes datos:

```
ndsconfig set n4u.nds.configdir custom_location
```

Windows

No es posible especificar una ubicación personalizada para los archivos de configuración en Windows.

3.3 Instalación por un usuario diferente de root

eDirectory 8.8 y las versiones posteriores admiten la instalación y configuración de servidores de eDirectory por parte de un usuario diferente de root. Las versiones anteriores de eDirectory podían ser instaladas y configuradas solamente por un usuario root con una sola instancia de eDirectory ejecutándose en un host.

Con eDirectory 8.8 o versiones superiores, un usuario diferente de root puede usar una compilación de archivo tar para instalar eDirectory. Puede haber varias instancias de instalaciones binarias de eDirectory realizadas por el mismo usuario o por usuarios diferentes. Sin embargo, incluso para las instalaciones non-root, los servicios a nivel de sistema como la Infraestructura de cifrado internacional de Novell (NICI), SNMP y SLP solo pueden instalarse con privilegios de root. NICI es un componente obligatorio y SNMP y SLP son componentes opcionales de la funcionalidad de eDirectory. Además, con una instalación de paquete, el usuario root solo puede instalar una instancia.

Después de la instalación, un usuario diferente de root puede configurar instancias del servidor de eDirectory por medio de la instalación del archivo tar individual o bien mediante una instalación binaria. Eso significa que puede haber varias instancias de servidores de eDirectory ejecutándose en un solo host porque cualquier usuario, ya sea root o non-root, puede configurar diferentes instancias de servidores de eDirectory en un solo host mediante instalación de paquete o de archivo tar. Para obtener información más detallada sobre la función de múltiples instancias, consulte [“Multiple Instances”](#) (Múltiples instancias) y [“Upgrading Multiple Instances”](#) (Actualización de múltiples instancias) en la [NetIQ eDirectory 8.8 SP8 Installation Guide](#).

La instalación y configuración por un usuario diferente de root solo se aplica a las plataformas Linux. Para obtener más información sobre la instalación y configuración por un usuario diferente de root, consulte [“Nonroot User Installing eDirectory 8.8”](#) (Instalación de eDirectory 8.8 por un usuario diferente de root) en la [NetIQ eDirectory 8.8 SP8 Installation Guide](#).

3.4 Compatibilidad mejorada para instalaciones en clústeres de alta disponibilidad

eDirectory 8.8 SP8 simplifica la instalación y la gestión de eDirectory tanto en clústeres de Linux y Windows, lo que mejora la compatibilidad de agrupación en clústeres y habilita la función de alta disponibilidad. eDirectory proporciona además alta disponibilidad a través de la sincronización de réplica, que puede combinarse con la agrupación en clúster para obtener una mayor disponibilidad.

Para obtener más información sobre la instalación de eDirectory en clústeres, consulte la [NetIQ eDirectory 8.8 SP8 Installation Guide](#).

3.5 Cumplimiento de estándares

eDirectory 8.8 cumple con las siguientes normas:

- ♦ [Sección 3.5.1, “Conformidad con FHS”, en la página 23](#)
- ♦ [Sección 3.5.2, “Conformidad con LSB”, en la página 24](#)

3.5.1 Conformidad con FHS

A fin de evitar conflictos con los archivos de aplicaciones de otros productos, eDirectory 8.8 sigue el estándar jerárquico del sistema de archivos (FHS). Esta función solo está disponible en Linux.

eDirectory sigue esta estructura de directorios solamente si ha elegido instalarla en la ubicación por defecto. Si ha elegido una ubicación personalizada, la estructura de directorios sería *custom_location/default_path*.

Por ejemplo, si elige instalar en el directorio `eDir88`, se seguiría la misma estructura de directorios en el directorio `eDir88`, igual que se instalarían las páginas man en el directorio `/eDir88/opt/novell/man`.

En la siguiente tabla se enumeran los cambios en la estructura de directorios:

Tipo de archivos almacenados en el directorio	Nombre y vía del directorio
Binarios ejecutables y guiones de shell estático	<code>/opt/novell/eDirectory/bin</code>
Binarios ejecutables para uso root	<code>/opt/novell/eDirectory/sbin</code>
Binarios de la biblioteca estática o dinámica	<code>/opt/novell/eDirectory/lib</code>
Archivos de configuración	<code>/etc/opt/novell/eDirectory/conf</code>
Datos dinámicos de lectura/escritura de tiempo de ejecución como la DIB	<code>/var/opt/novell/eDirectory/data</code>
Archivos de registro	<code>/var/opt/novell/eDirectory/log</code>
Páginas man de Linux	<code>/opt/novell/man</code>

Exportación de variables ambientales

Con la implementación de FHS en eDirectory 8.8, es necesario actualizar las variables ambientales de vía y exportarlas. Esto plantea los siguientes problemas:

- ♦ Debe recordar todas las vías exportadas, de manera que siempre que se abra un shell, deberá exportar estas vías y comenzar a usar las utilidades.
- ♦ Cuando desee utilizar más de un conjunto de binarios, deberá abrir más de un shell o tendrá que eliminar la definición y definir con frecuencia las vías en un conjunto de binarios diferente.

Para solucionar el problema anterior, puede usar el siguiente guión `/opt/novell/eDirectory/bin/ndspath`:

- ♦ Asigne el guión `ndspath` como prefijo a la utilidad y ejecute la utilidad deseada de la siguiente manera:

```
custom_location/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
```
- ♦ Exporte las vías en el shell actual de la siguiente manera:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```
- ♦ Después de introducir el comando anterior, ejecute las utilidades de la misma forma que lo haría normalmente. Invoque el guión de su perfil, `bashrc`, o guiones similares. Por lo tanto, siempre que entre o abra un nuevo shell, podrá comenzar a usar las utilidades directamente.

3.5.2 Conformidad con LSB

eDirectory 8.8 ahora cumple el estándar Linux Standard Base (LSB). LSB recomienda también cumplir el estándar FHS. Todos los paquetes de eDirectory en Linux tienen el prefijo *novell*. Por ejemplo, NDSserv ahora es *novell-NDSserv*.

3.6 Comprobaciones de actividad del servidor

eDirectory 8.8 introduce nuevas comprobaciones de la actividad del servidor que le ayudan a determinar si la actividad del servidor es segura antes de actualizar.

Las comprobaciones de actividad del servidor se ejecutan por defecto con cada actualización y se producen antes de la actualización del paquete en sí. No obstante, también puede ejecutar la herramienta de diagnóstico *ndscheck* para realizar las comprobaciones de actividad.

3.6.1 Necesidad de ejecutar comprobaciones de actividad

En las versiones anteriores de eDirectory, la actualización no verificaba la actividad del servidor antes de continuar con la actualización. Si el servidor era inestable, la operación de actualización fallaba y eDirectory tendría un estado incongruente. En algunos casos, es probable que no se pudiera revertir a la configuración anterior a la actualización.

Esta nueva herramienta de comprobación de la actividad soluciona este problema ya que permite asegurarse de que el servidor esté preparado para la actualización.

3.6.2 ¿Qué hace que un servidor tenga una actividad congruente?

La utilidad de comprobación de la actividad del servidor realiza varias [comprobaciones de la actividad](#) para estar seguro de que el árbol es congruente. El árbol se considera congruente cuando todas estas comprobaciones de la actividad finalizan de forma satisfactoria.

3.6.3 Realización de comprobaciones de la actividad

Puede realizar comprobaciones de la actividad del servidor de dos maneras:

- ♦ [“Con la actualización” en la página 24](#)
- ♦ [“Como utilidad independiente” en la página 25](#)

Nota: Debe tener derechos de administrador para poder ejecutar la utilidad de comprobación de la actividad. El derecho mínimo que se puede definir para ejecutar la utilidad es Público. Sin embargo, cuando se define el derecho Público, algunos objetos e información de partición del protocolo central NetWare (NCP) no están disponibles.

Con la actualización

Las comprobaciones de la actividad se ejecutan por defecto cada vez que se actualiza eDirectory.

Linux

Cada vez que se actualiza, se ejecutan por defecto las comprobaciones de la actividad antes de que comience la operación de actualización.

Para omitir las comprobaciones de la actividad, puede usar la opción `-j` con la utilidad `nds-install`.

Windows

Las comprobaciones de actividad del servidor se producen dentro del asistente de instalación. Puede habilitar o inhabilitar las comprobaciones de actividad cuando se le indique.

Como utilidad independiente

Puede ejecutar comprobaciones de actividad del servidor como utilidad independiente en cualquier momento que lo desee. En la siguiente tabla se explican las utilidades de comprobación de actividad.

Tabla 3-1 Utilidades de comprobación de actividad

Plataforma	Nombre de la utilidad
Linux	<code>ndscheck</code> Sintaxis: <code>ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path</code> Nota: Puede especificar <code>-h o --config-file</code> , pero no ambas opciones.
Windows	<code>ndscheck</code>

3.6.4 Tipos de comprobaciones de actividad

Al actualizar o ejecutar la utilidad `ndscheck`, se realizan las siguientes comprobaciones de actividad:

- ♦ [Actividad básica del servidor](#)
- ♦ [Actividad de particiones y de réplica](#)

Si ejecuta la utilidad `ndscheck`, los resultados de la comprobación de actividad se muestran en la pantalla y se registran en `ndscheck.log`. Para obtener más información sobre los archivos de registro, consulte la [Sección 3.6.6, “Archivos de registro”, en la página 27](#).

Si las comprobaciones de actividad se realizan dentro de la actualización, entonces, después de finalizar las comprobaciones de actividad, dependiendo de la gravedad del error, se le indicará que continúe el proceso de actualización o que lo cancele. En la [Sección 3.6.5, “Categorización de la actividad”, en la página 26](#) se describen los detalles del error.

Actividad básica del servidor

Esta es la primera etapa de la comprobación de actividad. La utilidad de comprobación de actividad comprueba los siguientes datos:

1. El servicio de eDirectory está en funcionamiento. La DIB está abierta y puede leer información básica del árbol como el nombre.
2. El servidor escucha en los números de puerto respectivos.

Para LDAP, obtiene los números de puerto TCP y SSL y comprueba si el servidor escucha en estos puertos.

De forma similar, obtiene los números de puerto HTTP y HTTPS y comprueba si el servidor escucha en estos puertos.

Actividad de particiones y de réplica

Después de comprobar la actividad básica del servidor, el siguiente paso consiste en comprobar la actividad de las particiones y la réplica de la siguiente manera:

1. Comprueba la actividad de las réplicas de las particiones locales.
2. Lee el anillo de réplica en cada una de las particiones alojadas por el servidor y comprueba si todos los servidores del anillo de réplica están en funcionamiento y todas las réplicas están en estado ACTIVADO.
3. Comprueba la sincronización horaria de todos los servidores del anillo de réplica. Esta muestra la diferencia horaria entre los servidores.

3.6.5 Categorización de la actividad

En función de los errores detectados mientras se comprobaba la actividad del servidor, puede haber tres categorías de actividad. El estado de las comprobaciones de actividad queda registrado en un archivo de registro. Para obtener más información, consulte la [Sección 3.6.6, "Archivos de registro", en la página 27](#).

Las tres categorías de actividad [Normal](#), [Advertencia](#) y [Crítico](#).

Normal

La actividad del servidor es normal cuando todas las comprobaciones de actividad se realizaron correctamente.

La actualización prosigue sin interrupciones.

Advertencia

La actividad del servidor esté en la categoría de advertencia cuando se detectan pequeños errores mientras se comprueba la actividad.

Si la comprobación de actividad se ejecuta dentro de la actualización, se preguntará si desea cancelar la operación o continuar.

Las advertencias se producen normalmente en las siguientes situaciones:

1. El servidor no escucha en los puertos LDAP y HTTP, ya sea en modo normal, seguro o ambos.

2. No es posible contactar con los servidores no maestros del anillo de réplica.
3. Los servidores del anillo de réplica no están sincronizados.

Crítico

La actividad del servidor es crítica cuando se detectan errores mientras se comprueba la actividad del servidor.

Si la comprobación de actividad se ejecuta dentro de la actualización, se cancela la operación de actualización.

La actividad crítica normalmente se produce en los siguientes casos:

1. No es posible leer o abrir la DIB. La DIB puede estar bloqueada o dañada.
2. No es posible contactar con todos los servidores del anillo de réplica.
3. Las particiones locales están ocupadas.
4. La réplica no se encuentra ACTIVADA.

3.6.6 Archivos de registro

Cada operación de comprobación de actividad del servidor, ya sea que se ejecute dentro de la actualización o como utilidad independiente, mantiene el estado de la actividad en un archivo de registro:

El contenido del archivo de registro es similar a los mensajes mostrados en la pantalla cuando se producen las comprobaciones.

El archivo de registro de comprobación de la actividad contiene la siguiente información:

- ♦ Estado de las comprobaciones de actividad (normal, advertencia y crítico).
- ♦ Las direcciones URL del sitio de asistencia de NetIQ.

En la siguiente tabla se presentan las ubicaciones de los archivos de registro en diversas plataformas:

Tabla 3-2 Ubicaciones del archivo de registro de comprobación de actividad

Plataforma	Nombre de archivo de registro	Ubicación del archivo de registro
Linux	<code>ndscheck.log</code> ,	<p>Depende de la ubicación especificada en la utilidad <code>ndscheck -F</code>.</p> <p>Si no utilizó la opción <code>-F</code>, la ubicación del archivo <code>ndscheck.log</code> se determina mediante las demás opciones que utilizó en la línea de comando <code>ndscheck</code> de la siguiente manera:</p> <ol style="list-style-type: none"> 1. Si utilizó la opción <code>-h</code>, el archivo <code>ndscheck.log</code> se guarda en el directorio de inicio del usuario. 2. Si utilizó la opción <code>--config-file</code>, el archivo <code>ndscheck.log</code> se guarda en el directorio de registro de la instancia del servidor. También puede seleccionar una instancia de la lista de múltiples instancias.

Plataforma	Nombre de archivo de registro	Ubicación del archivo de registro
Windows	ndscheck.log,	install_directory

3.7 Integración de SecretStore con eDirectory

eDirectory 8.8 le ofrece la opción de configurar Novell SecretStore 3.4 durante la configuración de eDirectory. Antes de eDirectory 8.8, era necesario instalar manualmente SecretStore.

SecretStore es una solución de gestión de contraseñas sencilla y segura. Permite utilizar una sola autenticación en eDirectory para acceder a la mayoría de aplicaciones de Linux, Windows, web y mainframe.

Una vez realizada la autenticación en eDirectory, las aplicaciones activadas para SecretStore almacenan y recuperan las credenciales de entrada apropiadas. Con SecretStore, se elimina la necesidad de recordar o sincronizar las diferentes contraseñas necesarias para acceder a las aplicaciones, los sitios web y los equipos mainframe protegidos mediante contraseña.

Para configurar SecretStore 3.4 junto con eDirectory, puede hacer lo siguiente:

- ♦ **Linux:**

Utilice el parámetro `ndsconfig add -m ss`. En este parámetro, `ss` se refiere a SecretStore y es un parámetro opcional. Si no menciona el nombre del módulo, se instalan todos los módulos. Si no desea configurar SecretStore, puede pasar el valor `no_ss` a esta opción especificando `-m no_ss`.

- ♦ **Windows:**

Al instalar eDirectory, existe una opción para especificar si desea configurar el módulo SecretStore. Por defecto, esta opción está seleccionada.

Para obtener más información sobre el uso de SecretStore, consulte la [Novell SecretStore 3.4 Administration Guide \(https://www.netiq.com/documentation/secretstore34/\)](https://www.netiq.com/documentation/secretstore34/) (Guía de administración de Novell SecretStore 3.4).

3.8 Instalación de Utilidades de eDirectory

Anteriormente, Utilidades de eDirectory formaba parte de Novell Audit. A partir de la versión eDirectory 8.8 SP3, Utilidades de eDirectory debe instalarse por separado.

Para obtener información detallada acerca de la instalación, configuración y desinstalación de Utilidades de eDirectory consulte la sección correspondiente en la [Guía de instalación de NetIQ eDirectory 8.8 SP8](#).

3.9 Información adicional

Consulte la siguiente documentación para obtener más información sobre cualquiera de las funciones tratadas en este capítulo.

- ♦ [Guía de instalación de NetIQ eDirectory 8.8 SP8](#)

- ♦ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8)
- ♦ En Linux: páginas `man nds-install`, `ndsconfig` y `ndscheck`

4 Copia de seguridad y recuperación de NICI

Novell International Cryptography Infrastructure (NICI) almacena claves y datos del usuario en el sistema de archivos y en directorios y archivos específicos del usuario y del sistema. Estos directorios y archivos están protegidos mediante el establecimiento de permisos adecuados para ellos utilizando el mecanismo facilitado por el sistema operativo. Esto lo realiza el programa de instalación de NICI.

La desinstalación de NICI del sistema no elimina los directorios y archivos del usuario o del sistema. Por tanto, la única razón para restaurar estos archivos a un estado anterior sería recuperarlos cuando se produce un fallo catastrófico del sistema o un error humano. Es importante entender que al sobrescribir un conjunto existente de directorios y archivos del usuario de NICI se podría alterar una aplicación existente.

La clave de la base de datos necesaria para abrir la DIB está codificada en las claves de NICI. Por tanto, si se realiza una copia de seguridad de eDirectory independientemente de la copia de seguridad de NICI entonces no sirve de nada.

Cambios con respecto al mecanismo anterior de copia de seguridad y restauración de NICI

Anteriormente, la copia de seguridad y restauración de NICI debía realizarse manualmente. En esta versión, se ha añadido una nueva solución de copia de seguridad y restauración de NICI. Se ha añadido un parámetro (-e) a la solución de copia de seguridad de eDirectory (copia de seguridad eMBox y DSBK) que permite:

1. Hacer una copia de seguridad de las claves de NICI cuando se ejecuta una copia de seguridad de eDirectory.
2. Restaurar las claves de NICI cuando se ejecuta una restauración de eDirectory.

Consulte “[Backing Up and Restoring NICI](#)” (Copia de seguridad y restauración de NICI) en la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

5 La utilidad ndspassstore

ndspassstore es una nueva utilidad que sirve para almacenar una contraseña cifrada para el usuario sadmin o el usuario de eDirectory. Esta utilidad está disponible en plataformas Linux y Windows. Esta utilidad toma el nombre de usuario y la contraseña como datos de entrada y los almacena en forma de pares de valores de clave cifrada.

En esta versión, la utilidad se utiliza para establecer la contraseña de sadmin.

Esta utilidad está disponible por defecto en C:\Novell\NDS en Windows y en /opt/novell/eDirectory/bin en Linux.

Sinopsis de comandos

Puede usar la utilidad ndspassstore introduciendo el siguiente comando en la consola del servidor:

```
ndspassstore -a <adminContext> -w <password>
```

Opción	Uso
-a adminContext	Esta opción se utiliza para aceptar el adminContext que es el nombre completo de un usuario con derechos administrativos.
-w contraseña	Esta opción se utiliza para aceptar la contraseña (contraseña de usuario) para la autenticación.

6 Múltiples instancias

Tradicionalmente, solo se podía configurar una instancia de NetIQ eDirectory en un único host. Con la función de múltiples instancias admitida en eDirectory 8.8, puede configurar lo siguiente:

- ♦ Múltiples instancias de eDirectory en un único host.
- ♦ Múltiples árboles en un único host.
- ♦ Múltiples réplicas del mismo árbol o partición en un único host.

eDirectory 8.8 también proporciona una utilidad ([ndsmanage](#)) que permite hacer un seguimiento fácil de las instancias.

La tabla siguiente enumera las plataformas que son compatibles con las múltiples instancias.

Función	Linux	Windows
Compatibilidad con múltiples instancias	✓	✗

En este capítulo se proporciona la siguiente información:

- ♦ [Sección 6.2, “Ejemplos de escenarios de implementación de múltiples instancias”](#), en la página 35
- ♦ [Sección 6.3, “Uso de múltiples instancias”](#), en la página 36
- ♦ [Sección 6.4, “Gestión de múltiples instancias”](#), en la página 37
- ♦ [Sección 6.5, “Ejemplo de escenario de múltiples instancias”](#), en la página 41
- ♦ [Sección 6.6, “Información adicional”](#), en la página 42

6.1 Necesidad de múltiples instancias

Las múltiples instancias surgieron de la necesidad de:

- ♦ Aprovechar el hardware de gama alta para configurar más de una instancia de eDirectory.
- ♦ Guiar su instalación en un único host antes de invertir en el hardware necesario.

6.2 Ejemplos de escenarios de implementación de múltiples instancias

Pueden utilizarse con eficacia múltiples instancias que pertenecen al mismo árbol o a varios árboles en los siguientes escenarios.

eDirectory en una empresa de gran tamaño

- ♦ En las grandes empresas, se puede proporcionar equilibrio de carga y alta disponibilidad de los servicios de eDirectory.

Por ejemplo, si tiene tres servidores de réplica ejecutando servicios LDAP en los puertos 1524, 2524 y 3524, respectivamente, puede configurar una nueva instancia de eDirectory y proporcionar un servicio de LDAP de alta disponibilidad en un nuevo puerto 636.

- ♦ Puede aprovechar el hardware de gama alta entre los departamentos de una organización configurando múltiples instancias en un único host.

eDirectory en una instalación de evaluación

- ♦ **Universidades:** muchos entusiastas (estudiantes) pueden evaluar eDirectory desde el mismo host utilizando las múltiples instancias.
- ♦ **Formación para administración de eDirectory:**
 - ♦ Los participantes pueden evaluar la administración utilizando las múltiples instancias.
 - ♦ Los instructores pueden usar un único host para impartir clase a los estudiantes. Cada estudiante puede tener su propio árbol.

6.3 Uso de múltiples instancias

eDirectory 8.8 hace que sea muy fácil configurar varias instancias. Para utilizar múltiples instancias de manera eficiente, es necesario planificar la instalación y luego configurar las múltiples instancias.

- ♦ [Sección 6.3.1, “Planificación de la instalación”, en la página 36](#)
- ♦ [Sección 6.3.2, “Configuración de múltiples instancias”, en la página 36](#)

6.3.1 Planificación de la instalación

Para poder usar esta función de manera eficiente, se recomienda planificar las instancias de eDirectory y garantizar que cada una tenga identificadores de instancia concretos como el nombre de host, el número de puerto, el nombre de servidor o el archivo de configuración.

Mientras se configuran múltiples instancias, es necesario asegurarse de que se ha planificado lo siguiente:

- ♦ Ubicación del archivo de configuración
- ♦ Ubicación de los datos variables (como los archivos de registro)
- ♦ Ubicación de la DIB
- ♦ Interfaz NCP™, puerto de identificación exclusiva para cada instancia y puertos de otros servicios (como LDAP, LDAPS, HTTP y el puerto HTTP seguro)
- ♦ Nombre de servidor exclusivo de cada instancia

6.3.2 Configuración de múltiples instancias

Puede configurar múltiples instancias de eDirectory mediante la utilidad `ndsconfig`. En la siguiente tabla se enumeran las opciones de `ndsconfig` que necesita incluir para configurar múltiples instancias.

Nota: Todas las instancias comparten la misma clave de servidor (NICI).

Opción	Descripción
--config-file	Especifica la vía absoluta y el nombre de archivo para almacenar el archivo de configuración <code>nds.conf</code> . Por ejemplo, para almacenar el archivo de configuración en el directorio <code>/etc/opt/novell/eDirectory/</code> , utilice <code>--config-file /etc/opt/novell/eDirectory/nds.conf</code> .
-b	Especifica el número de puerto en el que debe escuchar la nueva instancia. Nota: <code>-b</code> y <code>-B</code> se utilizan de forma exclusiva.
-B	Especifica el número de puerto junto con la dirección IP o la interfaz. Por ejemplo: <code>-B eth0@524</code> O bien <code>-B 100.1.1.2@524</code> Nota: <code>-b</code> y <code>-B</code> se utilizan de forma exclusiva.
-D	Crea los directorios <code>data</code> , <code>dib</code> y <code>log</code> en la vía especificada para la nueva instancia.
S	Especifica el nombre del servidor.

Al usar las opciones mencionadas anteriormente, puede configurar una nueva instancia de eDirectory.

También puede configurar una nueva instancia mediante la utilidad `ndsmanage`. Para obtener más información, consulte la [“Creación de una instancia a través de `ndsmanage`”](#) en la página 38.

6.4 Gestión de múltiples instancias

En esta sección se incluye la información siguiente:

- ♦ [Sección 6.4.1, “La utilidad `ndsmanage`”, en la página 37](#)
- ♦ [Sección 6.4.2, “Identificación de una instancia específica”, en la página 41](#)
- ♦ [Sección 6.4.3, “Invocar una utilidad para una instancia específica”, en la página 41](#)

6.4.1 La utilidad `ndsmanage`

La utilidad `ndsmanage` permite hacer lo siguiente:

- ♦ [Enumerar las instancias configuradas](#)
- ♦ [Crear una nueva instancia](#)
- ♦ [Realizar lo siguiente para una instancia seleccionada:](#)
 - ♦ Enumerar las réplicas del servidor
 - ♦ Iniciar la instancia

- ♦ Detener la instancia
- ♦ Ejecutar DSTrace (ndstrace) para la instancia
- ♦ Desconfigurar la instancia
- ♦ [Iniciar y detener todas las instancias](#)

Listado de instancias

En la siguiente tabla se describe cómo enumerar las instancias de eDirectory.

Tabla 6-1 Uso de `ndsmanage` para enumerar las instancias

Sintaxis	Descripción
<code>ndsmanage</code>	Enumera todas las instancias configuradas por usted.
<code>ndsmanage -a --all</code>	Enumera las instancias de todos los usuarios que utilizan una instalación particular de eDirectory.
<code>ndsmanage nombreusuario</code>	Enumera las instancias configuradas por un usuario específico

Los siguientes campos se muestran para cada instancia:

- ♦ Vía al archivo de configuración
- ♦ Nombre completo del servidor y puerto
- ♦ Estado (si la instancia está activa o inactiva)

Nota: Esta utilidad enumera todas las instancias configuradas para un solo binario.

Consulte [Figura 6-1 en la página 38](#) para obtener más información.

Creación de una instancia a través de `ndsmanage`

Para crear una nueva instancia a través de `ndsmanage`:

- 1 Introduzca el siguiente comando:

```
ndsmanage
```

Si ha configurado dos instancias, se muestra la siguiente pantalla:

Figura 6-1 Pantalla de salida de la utilidad `ndsmanage`

```
root@MYSOL-8 / $ ndsmanage

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@524 : ACTIVE

[2] /builds/server2/eDirectory/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@1525 : ACTIVE

Enter [1 - 2] for more options, [c] for creating a new instance or [q] to quit: █
```

2 Introduzca c para crear una nueva instancia.

Puede crear un nuevo árbol o añadir un servidor a un árbol existente. Siga las instrucciones de la pantalla para crear una nueva instancia.

Realización de operaciones para una instancia específica

Puede realizar las siguientes operaciones para cada instancia:

- ♦ “Inicio de una instancia específica” en la página 39
- ♦ “Detención de una instancia específica” en la página 39
- ♦ “Desconfiguración de una instancia” en la página 40

Aparte de las enumeradas anteriormente, también puede ejecutar DTrace para una instancia seleccionada.

Inicio de una instancia específica

Para iniciar una instancia configurada por usted, realice los siguientes pasos:

1 Indique lo siguiente:

```
ndsmanage
```

2 Seleccione la instancia que desea iniciar.

El menú se amplía para incluir las opciones que puede realizar en una instancia específica.

Figura 6-2 Pantalla de salida de la utilidad `ndsmanage` con opciones de instancia

```
root@mysol-8 / $ ndsmanage root

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@524 : ACTIVE

[2] /builds/server2/eDirectory/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@1525 : ACTIVE

Enter [1 - 2] for more options, [c] for creating a new instance or [q] to quit: 1
[l] List the replicas on the server
[s] Start the instance
[k] Stop the instance
[t] Run ndstrace
[d] Deconfigure
[q] Quit
What do you want to do with this instance? [ Choose from above]: █
```

3 Introduzca s para iniciar la instancia.

Opcionalmente, puede introducir lo siguiente en la línea de comandos:

```
ndsmanage start --config-file configuration_file_of_the_instance_configured_by_you
```

Detención de una instancia específica

Para detener una instancia configurada por usted, realice lo siguiente:

1 Indique lo siguiente:

```
ndsmanage
```

- 2 Seleccione la instancia que desea detener.

El menú se amplía para incluir las opciones que puede realizar en una instancia específica. Para obtener más información, consulte la [Pantalla de salida de la utilidad ndsmanage con opciones de instancia \(en la página 39\)](#).

- 3 Introduzca `k` para detener la instancia.

Opcionalmente, también puede introducir lo siguiente en la línea de comandos:

```
ndsmanage stop --config-file configuration_file_of_the_instance_configured_by_you
```

Desconfiguración de una instancia

Para desconfigurar una instancia, haga lo siguiente:

- 1 Indique lo siguiente:

```
ndsmanage
```

- 2 Seleccione la instancia que desea desconfigurar.

El menú se amplía para incluir las opciones que puede realizar en una instancia específica. Para obtener más información, consulte la [Pantalla de salida de la utilidad ndsmanage con opciones de instancia \(en la página 39\)](#).

- 3 Introduzca `d` para desconfigurar la instancia.

Inicio y detención de todas las instancias

Puede iniciar y detener todas las instancias que ha configurado.

Inicio de todas las instancias

Para iniciar todas las instancias configuradas que ha configurado, introduzca lo siguiente en la línea de comandos:

```
ndsmanage startall
```

Para iniciar una instancia específica, consulte [“Inicio de una instancia específica” en la página 39](#).

Detención de todas las instancias

Para detener todas las instancias que ha configurado, introduzca lo siguiente en la línea de comandos:

```
ndsmanage stopall
```

Para detener una instancia específica, consulte [“Detención de una instancia específica” en la página 39](#).

6.4.2 Identificación de una instancia específica

Al configurar múltiples instancias, asigna un nombre de host, un número de puerto y una vía al archivo de configuración exclusiva para cada instancia. Este nombre de host y número de puerto son los identificadores de instancia.

La mayoría de las utilidades tienen la opción `-h hostname:port` o `--config-file configuration_file_location` que permite especificar una instancia en particular. Consulte las páginas man de las utilidades para obtener más información.

6.4.3 Invocar una utilidad para una instancia específica

Si desea ejecutar una utilidad para una instancia específica, debe incluir el identificador de la instancia en el comando de la utilidad. Los identificadores de la instancia son la vía al archivo de configuración y el nombre de host y el número de puerto. Para hacerlo puede usar la opción `--config-file configuration_file_location` o `-h hostname:port`.

Si no incluye los identificadores de instancia en el comando, la utilidad muestra las diversas instancias que son de su propiedad y le indica que seleccione la instancia para la que desea ejecutar la utilidad.

Por ejemplo, para ejecutar DTrace para una utilidad específica utilizando la opción `--config-file`, se indicaría lo siguiente:

```
ndstrace --config-file configuration_filename_with_location
```

6.5 Ejemplo de escenario de múltiples instancias

Maria es un usuario diferente de root que desea configurar dos árboles en un único host para un único binario.

6.5.1 Planificación de la instalación

Mary especifica los siguientes identificadores de instancia.

♦ **Instancia n.º 1:**

Número de puerto en el que la instancia debe escuchar	1524
Vía al archivo de configuración	/home/maryinst1/nds.conf
Directorio DIB	/home/mary/inst1/var

♦ **Instancia n.º 2:**

Número de puerto en el que la instancia debe escuchar	2524
Vía al archivo de configuración	/home/mary/inst2/nds.conf
Directorio DIB	/home/mary/inst2/var

6.5.2 Configuración de las instancias

Para configurar las instancias basadas en los identificadores de instancia mencionados, María deben introducir los siguientes comandos.

- ♦ **Instancia n.º 1:**

```
ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D  
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

- ♦ **Instancia n.º 2:**

```
ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D  
/home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
```

6.5.3 Invocar una utilidad para una instancia

Si María desea ejecutar la utilidad DTrace para la instancia n.º 1 que está escuchando en el puerto 1524, con su archivo de configuración en `/home/mary/inst1/nds.conf` su archivo DIB en `/home/mary/inst1/var`, entonces puede ejecutar la utilidad de la siguiente manera:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

O bien

```
ndstrace -h 164.99.146.109:1524
```

Si María no especifica los identificadores de instancia, la utilidad muestra todas las instancias de María y le pide que seleccione una instancia.

6.5.4 Listado de las instancias configuradas

Si María desea conocer detalles acerca de las instancias que hay en el host, puede ejecutar la utilidad `ndsmanage`.

- ♦ Para mostrar todas las instancias de María:

```
ndsmanage
```

- ♦ Para mostrar todas las instancias de Juan (nombre de usuario es Juan):

```
ndsmanage john
```

- ♦ Para mostrar todas las instancias de todos los usuarios que utilizan una determinada instalación de eDirectory:

```
ndsmanage -a
```

6.6 Información adicional

Consulte los siguientes documentos para obtener más información sobre la compatibilidad con múltiples instancias:

- ♦ [Guía de instalación de NetIQ eDirectory 8.8 SP8](#)
- ♦ Para Linux: páginas `man` de `ndsconfig` y `ndsmanage`

7 Autenticación en eDirectory a través de SASL GSSAPI

El mecanismo SASL GSSAPI para NetIQ eDirectory 8.8 permite autenticarse en eDirectory a través de LDAP con un ticket de Kerberos y sin necesidad de introducir la contraseña de usuario de eDirectory. El ticket Kerberos debe obtenerse autenticándose en un servidor Kerberos.

Esta función es muy útil para los usuarios de aplicaciones de LDAP en entornos que ya tienen implementada una infraestructura de Kerberos. Por lo tanto, estos usuarios deben ser capaces de autenticarse en el servidor LDAP sin proporcionar una contraseña de usuario LDAP independiente.

Para facilitar esto, eDirectory presenta el mecanismo SASL GSSAPI.

La implementación actual de SASL GSSAPI es compatible con [RFC 2222](http://www.ietf.org/rfc/rfc2222.txt?number=2222) (<http://www.ietf.org/rfc/rfc2222.txt?number=2222>) y admite sólo Kerberos v5 como mecanismo de autenticación.

En este capítulo se proporciona la siguiente información:

- ♦ [Sección 7.1, “Conceptos”, en la página 43](#)
- ♦ [Sección 7.2, “¿Cómo funciona GSSAPI con eDirectory?”, en la página 44](#)
- ♦ [Sección 7.3, “Configuración de GSSAPI”, en la página 45](#)
- ♦ [Sección 7.4, “¿Cómo utiliza LDAP GSSAPI?”, en la página 45](#)
- ♦ [Sección 7.5, “Términos comunes”, en la página 46](#)

7.1 Conceptos

- ♦ [Sección 7.1.1, “¿Qué es Kerberos?”, en la página 43](#)
- ♦ [Sección 7.1.2, “¿Qué es SASL?”, en la página 44](#)
- ♦ [Sección 7.1.3, “¿Qué es GSSAPI?”, en la página 44](#)

7.1.1 ¿Qué es Kerberos?

Kerberos es un protocolo estándar que proporciona un medio de autenticación de entidades en una red. Se basa en un modelo de terceros de confianza. Implica secretos compartidos y utiliza la criptografía de claves simétricas.

Para obtener más información, consulte [RFC 1510](http://www.ietf.org/rfc/rfc1510.txt?number=1510) (<http://www.ietf.org/rfc/rfc1510.txt?number=1510>).

7.1.2 ¿Qué es SASL?

Simple Authentication and Security Layer (SASL) proporciona una capa de abstracción de autenticación para las aplicaciones. Es un entorno al que se pueden conectar a los módulos de autenticación.

Para obtener más información, consulte RFC 2222 (<http://www.ietf.org/rfc/rfc2222.txt?number=2222>).

7.1.3 ¿Qué es GSSAPI?

Generic Security Services Application Program Interface (GSSAPI) proporciona autenticación y otros servicios de seguridad a través de un conjunto estándar de APIs. Es compatible con mecanismos de autenticación diferentes. Kerberos v5 es el más común.

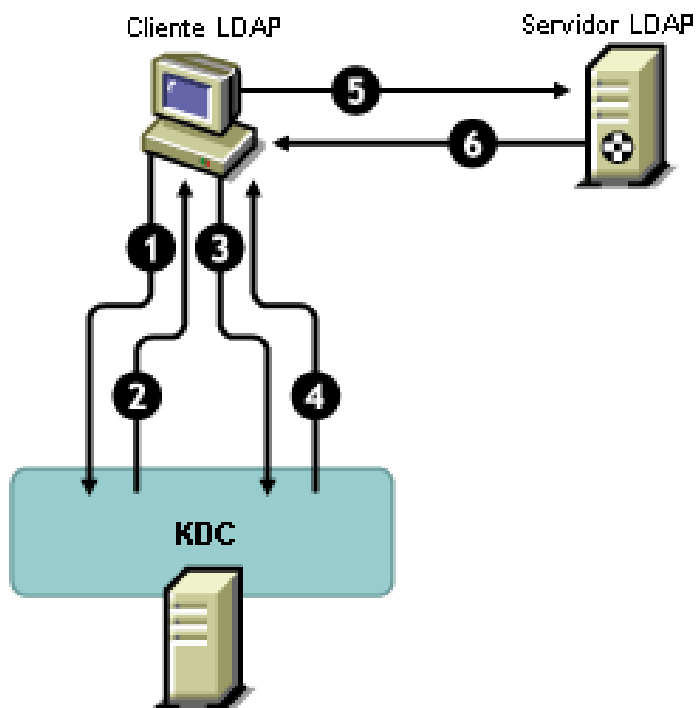
Para obtener más información sobre las API GSS, consulte RFC 1964 (<http://www.ietf.org/rfc/rfc1964.txt?number=1964>).

Esta implementación de SASL GSSAPI es de la sección 7.2 de RFC 2222 (<http://www.ietf.org/rfc/rfc2222.txt?number=2222>).

7.2 ¿Cómo funciona GSSAPI con eDirectory?

El siguiente diagrama ilustra cómo funciona la GSSAPI con un servidor LDAP.

Figura 7-1 ¿Cómo funciona GSSAPI?



En la figura anterior, los números indican lo siguiente:

- 1 Un usuario de eDirectory envía una solicitud a través de un cliente LDAP al servidor KDC Kerberos (centro de distribución de claves) de un ticket inicial denominado un ticket de concesión de tickets (TGT).

- Puede ser un KDC Kerberos de MIT o Microsoft*.
- 2 KDC responde al cliente LDAP con un TGT.
 - 3 El cliente LDAP devuelve el TGT al KDC y solicita un ticket de servicio de LDAP.
 - 4 KDC responde al cliente LDAP con el ticket de servicio de LDAP.
 - 5 El cliente LDAP realiza un `ldap_sasl_bind` con el servidor LDAP y envía el ticket de servicio de LDAP.
 - 6 El servidor LDAP valida el ticket de servicio de LDAP con la ayuda del mecanismo GSSAPI y, basándose en el resultado, devuelve un `ldap_sasl_bind` satisfactorio o un error al cliente LDAP.

7.3 Configuración de GSSAPI

- 1 El módulo auxiliar (plug-in) para SASL-GSSAPI de iManager no funcionará si iManager no está configurado para usar conexión de SSL/TLS para eDirectory. Se requiere una conexión segura para proteger la clave principal del dominio y las claves de principal.

Por defecto, iManager normalmente está configurado para la conexión SSL/TLS para eDirectory. Si desea configurar el método de entrada de Kerberos para GSSAPI en un árbol distinto del que aloja la configuración iManager, necesitará configurar iManager para conexión SSL/TLS para eDirectory.

Para obtener información acerca de cómo configurar iManager con conexión SSL/TLS para eDirectory, consulte la *NetIQ iManager 2.7 Administration Guide* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html) (Guía de administración de iManager 2.7).

El plug-in de SASL-GSSAPI (`kerberosPlugin.npm`) está disponible tanto en el archivo `eDir_88_iMan26_Plugins.npm` como en `eDir_88_iMan27_Plugins.npm`. Descargue los NPM del [sitio Web de descargas de Novell](http://download.novell.com) (<http://download.novell.com>).

- 2 Para utilizar un ticket Kerberos para autenticar un servidor eDirectory:
 - 2a Amplíe el esquema de Kerberos.
 - 2b Cree un contenedor de dominio.
 - 2c Extraiga una clave compartida o de clave Principal de servicio del KDC.
 - 2d Cree el objeto Principal del servicio LDAP.
 - 2e Asocie un nombre principal de Kerberos con el objeto de usuario.

Para obtener información sobre los pasos anteriores, consulte “[Configuring GSSAPI with eDirectory](#)” (Configuración de GSSAPI con eDirectory) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

7.4 ¿Cómo utiliza LDAP GSSAPI?

Después de configurar GSSAPI, se agrega junto con los otros métodos SASL al atributo de `supportedSASLMechanisms` en `rootDSE.rootDSE` (entrada específica de DSA [Directory System Agent]) es una entrada que se encuentra en la raíz del árbol de información de directorio

(DIT). Para obtener más información, consulte [“Understanding How LDAP Works with eDirectory”](#) (Comprender cómo funciona LDAP con eDirectory) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

El servidor LDAP consulta SASL para los mecanismos instalados cuando obtiene su configuración y admite automáticamente lo que está instalado. El servidor LDAP también informa de los mecanismos actuales de SASL compatibles en su `rootDSE` con el atributo `supportedSASLMechanisms`.

Por lo tanto, al configurar GSSAPI, se convierte en el mecanismo predeterminado. Sin embargo, para realizar específicamente una operación de LDAP a través del mecanismo SASL GSSAPI, puede mencionar GSSAPI en la línea de comandos.

Por ejemplo, para realizar una búsqueda en OpenLDAP utilizando el mecanismo de GSSAPI, escribiría lo siguiente:

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

7.5 Términos comunes

La tabla siguiente define las terminologías utilizadas frecuentemente con Kerberos y GSSAPI.

Tabla 7-1 Terminología de Kerberos/GSSAPI

Término	Definición
Centro de distribución de claves (KDC)	Servidor Kerberos que autentica usuarios y emite tickets.
Principal	Entidad (usuario o instancia de servicio) registrada en el KDC.
Dominio	Dominio o grupo de identificadores principales facilitados por un conjunto de KDCs.
Ticket de servicio (ST)	Registro que contiene la información del cliente, información de servicio y una clave de sesión que se cifra con la clave compartida del identificador principal del servicio en concreto.
Ticket de concesión de tickets (TGT)	Tipo de ticket con el que el cliente puede obtener tickets adicionales de Kerberos.

8 Aplicación de contraseñas universales que diferencian mayúsculas de minúsculas

En NetIQ eDirectory 8.8, puede habilitar el uso de una contraseña universal y que su contraseña diferencie mayúsculas de minúsculas cuando acceda al servidor de eDirectory 8.8 a través de las utilidades y los clientes siguientes:

- ♦ Novell Client 4.9 y posterior
- ♦ Utilidades de administración actualizadas a eDirectory 8.8
- ♦ NetIQ iManager 2.7 y versiones posterior, excepto cuando se está ejecutando en Windows

Puede utilizar cualquier versión del SDK de LDAP con contraseñas que distinguen entre mayúsculas y minúsculas.

La tabla siguiente muestra las plataformas en las que se admite la función de contraseña que distingue entre mayúsculas y minúsculas:

Función	Linux	Windows
Aplicación de contraseña universal que distingue mayúsculas de minúsculas	✓	✓

En este capítulo se proporciona la siguiente información:

- ♦ [Sección 8.1, “Necesidad de contraseñas que distinguen mayúsculas de minúsculas”, en la página 47](#)
- ♦ [Sección 8.2, “Cómo hacer que la contraseña distinga mayúsculas de minúsculas”, en la página 48](#)
- ♦ [Sección 8.3, “Actualización de las utilidades y los clientes heredados de Novell”, en la página 49](#)
- ♦ [Sección 8.4, “Cómo impedir que los clientes heredados de Novell accedan al servidor de eDirectory 8.8.”, en la página 50](#)
- ♦ [Sección 8.5, “Información adicional”, en la página 55](#)

8.1 Necesidad de contraseñas que distinguen mayúsculas de minúsculas

Hacer que las contraseñas distingan entre mayúsculas y minúsculas potencia la seguridad de acceso al directorio. Por ejemplo, si tiene una contraseña aBc que distingue mayúsculas de minúsculas, todas las pruebas de entrada con las combinaciones abc o Abc o ABC generarían un error.

En eDirectory 8.8 y versiones posteriores, puede hacer que las contraseñas distingan entre mayúsculas y minúsculas para todos los clientes se actualizan a eDirectory 8.8.

Al exigir el uso de contraseñas que distinguen entre mayúsculas y minúsculas, puede impedir que los clientes heredados de Novell tengan acceso al servidor de eDirectory 8.8. Consulte [Sección 8.4, “Cómo impedir que los clientes heredados de Novell accedan al servidor de eDirectory 8.8.”](#), en la [página 50](#) para obtener más información.

8.2 Cómo hacer que la contraseña distinga mayúsculas de minúsculas

En eDirectory 8.8 y versiones posteriores, puede hacer que las contraseñas distingan entre mayúsculas y minúsculas para todos los clientes habilitando la contraseña universal. Por defecto, la contraseña universal está inhabilitada.

8.2.1 Requisitos previos

Por defecto, LDAP y otras utilidades del servidor utilizan primero la entrada NDS y si ésta falla, utilice la entrada con contraseña simple. Para poder aplicar la función de contraseña que distingue mayúsculas de minúsculas, la entrada debe realizarse a través de Servicios NMAS (autenticación modular) de Novell. Por lo tanto, deberá establecer la variable de entorno `NDS_TRY_NMASLOGIN_FIRST` en `true` para disponer de la función de contraseña que distingue mayúsculas de minúsculas.

Realice el procedimiento siguiente para disponer de la función de contraseña que distingue mayúsculas de minúsculas:

- 1 Defina la variable de entorno

- ♦ Linux:

Agregue lo siguiente en `/opt/novell/eDirectory/sbin/pre_ndsd_start` al final.

```
NDS_TRY_NMASLOGIN_FIRST=true
export NDS_TRY_NMASLOGIN_FIRST
```

- ♦ Windows:

Haga clic con el botón derecho en Mi PC y seleccione Propiedades. En la ficha Avanzadas, haga clic en Variables de entorno. En Variables del sistema, agregue la variable y establezca el valor en `true`.

- 2 Reinicie el servidor eDirectory.

Nota: El uso de NMAS para la autenticación aumenta el tiempo de entrada.

8.2.2 Cómo hacer que la contraseña distinga mayúsculas de minúsculas

- 1 Entre en eDirectory mediante la contraseña existente.

En el caso de una instalación nueva, la contraseña existente es la que se establece durante la configuración de eDirectory 8.8.

Por ejemplo, la contraseña es "novell".

Nota: Esta contraseña no hace distinción entre mayúsculas y minúsculas.

- 2 Habilitar Contraseña Universal.

Para obtener más información, consulte la sección “Deploying Universal Password” (Implementación de una contraseña universal) en la *Novell Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guía de administración de Novell Password Management 3.3).

3 Salga de la sesión de eDirectory.

4 Acceda a eDirectory mediante la contraseña existente utilizando mayúsculas o minúsculas como desee.

La contraseña que facilite ahora distinguirá entre mayúsculas y minúsculas.

Por ejemplo, escriba "NoVELL".

Ahora, la contraseña es "NoVELL". Por lo tanto, "novell" o cualquier combinación de mayúsculas alternativa que no sea "NoVELL" podría no ser válida.

Si va a migrar a las contraseñas que distinguen entre mayúsculas y minúsculas, consulte la [Sección 8.3.1, “Migración a contraseñas que distinguen entre mayúsculas y minúsculas”, en la página 50.](#)

Cualquier nueva contraseña que defina distinguirá entre mayúsculas y minúsculas dependiendo de en qué nivel (objeto o partición) se haya habilitado la contraseña universal.

8.2.3 Gestión de contraseñas que distinguen entre mayúsculas y minúsculas

Puede gestionar la función que distingue entre mayúsculas y minúsculas de las contraseñas, habilitando o inhabilitando la contraseña universal a través de iManager. Para obtener más información, consulte la sección “Deploying Universal Password” (Implementación de una contraseña universal) de la *NetIQ Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guía de administración de NetIQ Password Management 3.3)..

8.3 Actualización de las utilidades y los clientes heredados de Novell

A continuación se indican las versiones más recientes de los clientes de Novell y de las utilidades de NetIQ:

- ♦ Novell Client4.9
- ♦ Utilidades de administración con eDirectory 8.8
- ♦ NetIQ iManager 2.7 y versiones posteriores

Los clientes y las utilidades anteriores a las versiones mencionadas son los clientes heredados de Novell.

Puede tener contraseñas que distinguen entre mayúsculas y minúsculas para los clientes de Novell heredados después de actualizarlos a sus versiones más recientes. eDirectory 8.8 facilita la migración de las contraseñas existentes a las contraseñas que distinguen entre mayúsculas y minúsculas de manera flexible. Consulte [Sección 8.3.1, “Migración a contraseñas que distinguen entre mayúsculas y minúsculas”, en la página 50](#) para obtener más información.

En caso de que no se actualicen los clientes heredados a sus versiones más recientes, estos clientes pueden bloquearse para que no puedan usar eDirectory 8.8 en el servidor. Consulte [Sección 8.4, “Cómo impedir que los clientes heredados de Novell accedan al servidor de eDirectory 8.8.”](#), en la [página 50](#) para obtener más información.

8.3.1 Migración a contraseñas que distinguen entre mayúsculas y minúsculas

La contraseña universal está inhabilitada por defecto y, por lo tanto, las contraseñas existentes no se verán afectadas hasta que habilite la contraseña universal en iManager. Si desea obtener instrucciones detalladas, consulte la [Sección 8.2, “Cómo hacer que la contraseña distinga mayúsculas de minúsculas”](#), en la [página 48](#).

En el ejemplo siguiente se explica la migración a contraseñas que distinguen entre mayúsculas y minúsculas:

Sesión de entrada 1: la contraseña universal está inhabilitada por defecto.

- ♦ Se entra con la contraseña existente. Por ejemplo, supongamos que su contraseña es netiq.
- ♦ Esta contraseña no hace distinción entre mayúsculas y minúsculas. Por lo tanto, netiq y NetIQ son contraseñas válidas.
- ♦ Después de entrar, se habilita la contraseña universal. Consulte la sección [“Deploying Universal Password” \(Implementación de una contraseña universal\) de la NetIQ Password Management 3.3 Administration Guide](#) (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guía de administración de NetIQ Password Management 3.3).

Sesión de entrada 2: la contraseña universal está habilitada por defecto.

- ♦ Se entra con la contraseña existente. Por ejemplo, supongamos que escribe la contraseña como noVell.
- ♦ Cuando está habilitada la contraseña universal, esta contraseña distingue entre mayúsculas y minúsculas. Por ello, debe recordar cómo ha escrito la contraseña en este momento.

Sesión de entrada n.º 3 e inicios de sesión posteriores.

- ♦ Si entra con la contraseña netIQ, es válida.
- ♦ Si entra con la contraseña NetIQ (o cualquier otra versión excepto noVell), no será válida.

8.4 Cómo impedir que los clientes heredados de Novell accedan al servidor de eDirectory 8.8.

En eDirectory 8.7.1 y 8.7.3, podía evitar que los clientes heredados de Novell [definieran o cambiaran](#) la contraseña NDS. Con eDirectory 8.8, también puede evitar que entren en eDirectory 8.8 y comprueben las contraseñas.

Para permitir o no permitir a los clientes heredados de Novell el uso de eDirectory 8.8, necesitará configurar la entrada de NDS a través iManager o LDAP.

En esta sección se incluye la información siguiente:

- ♦ [Sección 8.4.1, “Necesidad de evitar que los clientes heredados de Novell accedan al servidor de eDirectory 8.8”](#), en la [página 51](#)

- ♦ [Sección 8.4.2, “Gestión de las configuraciones de entrada de NDS”, en la página 51](#)
- ♦ [Sección 8.4.3, “Operaciones de partición”, en la página 55](#)
- ♦ [Sección 8.4.4, “Aplicación de contraseñas que distinguen mayúsculas de minúsculas en un árbol mixto”, en la página 55](#)

8.4.1 Necesidad de evitar que los clientes heredados de Novell accedan al servidor de eDirectory 8.8

Las contraseñas de los clientes heredados de Novell no distinguen mayúsculas de minúsculas. Por lo tanto, en eDirectory 8.8 y versiones posteriores, cuando desee imponer el uso de contraseñas que distinguen mayúsculas de minúsculas, deberá bloquear el acceso por parte de los clientes heredados al directorio.

En versiones anteriores a Novell Client 4.9, la contraseña universal no era compatible. Esto sucedía porque los cambios de entrada y contraseña se implementaban directamente en la contraseña de NDS en lugar de en NMAS. Ahora, si utiliza la contraseña universal, cambiar las contraseñas a través de los clientes heredados puede crear un problema llamado "deriva de contraseña". Esto significa que las contraseñas de NDS y universal no están sincronizadas. Para evitar este problema, una opción es bloquear los cambios de contraseña de los clientes anteriores a la versión 4.9.

Consulte la siguiente sección, [Gestión de las configuraciones de entrada de NDS](#), para obtener más información acerca de cómo bloquear el acceso por parte de los clientes heredados al servidor de eDirectory 8.8.

8.4.2 Gestión de las configuraciones de entrada de NDS

Al configurar la entrada de NDS, puede permitir o no permitir el acceso por parte de los clientes heredados de Novell al servidor de eDirectory 8.8. Puede gestionar las configuraciones de entrada de NDS mediante iManager 2.6 y LDAP.

En eDirectory 8.8 y versiones posteriores, puede configurar la configuración y el cambio de contraseñas a través de LDAP como de iManager.

Esta sección contiene información sobre lo siguiente:

- ♦ [“Configuraciones de NDS en diferentes niveles” en la página 51](#)
- ♦ [“Gestión de configuraciones de NDS mediante iManager” en la página 53](#)
- ♦ [“Gestión de configuraciones de NDS a través de LDAP” en la página 53](#)
- ♦ [Sección 8.4.4, “Aplicación de contraseñas que distinguen mayúsculas de minúsculas en un árbol mixto”, en la página 55](#)

Configuraciones de NDS en diferentes niveles

Puede configurar la entrada de NDS en uno o todos los siguientes niveles:

- ♦ Nivel de partición
- ♦ Nivel de objeto

Si no se especifica la configuración en ninguno de los niveles, la configuración de entrada de NDS se habilita en todos los niveles.

La configuración de nivel de objeto siempre reemplaza la configuración a nivel de partición. La tabla siguiente describe cada uno de los métodos:

Tabla 8-1 Configuración de NDS

Configuración a nivel de objeto	Configuración a nivel de partición	Configuración
No especificado	Habilitado	Habilitado
Habilitado	No especificado	Habilitado
No especificado	Inhabilitado	Inhabilitado
Inhabilitado	No especificado	Inhabilitado
Habilitado	Habilitado	Habilitado
Habilitado	Inhabilitado	Habilitado
Inhabilitado	Habilitado	Inhabilitado
Inhabilitado	Inhabilitado	Inhabilitado

En todos los niveles (objeto y partición) se puede configurar la entrada de NDS para lo siguiente:

- ♦ Entrar en el directorio utilizando una contraseña NDS o comprobar la contraseña NDS
- ♦ Establecer una nueva contraseña y cambiar la contraseña existente

Entrada en el directorio o comprobación de la contraseña NDS

La entrada y la verificación de la contraseña significa:

- ♦ Acceder al directorio utilizando una contraseña NDS.
- ♦ Verificar la contraseña existente en el directorio.

La entrada/verificación de la contraseña NDS está habilitada por defecto. Cuando se inhabilita la clave de entrada/verificación, no podrá entrar en la versión más reciente de eDirectory ni verificar las contraseñas. Puede habilitar o deshabilitar la entrada/verificación de la contraseña NDS en los niveles de la partición y el objeto. Si se inhabilita la entrada/verificación, no podrá [configurar ni cambiar las contraseñas de NDS](#).

Puede configurar la entrada/verificación de la contraseña NDS a través de iManager y LDAP. Para obtener más información, consulte la [“Gestión de configuraciones de NDS mediante iManager”](#) en la página 53 y la [“Gestión de configuraciones de NDS a través de LDAP”](#) en la página 53.

Definición de una nueva contraseña o cambio de la contraseña NDS

Definir o cambiar una contraseña de NDS significa

- ♦ Establecer una nueva contraseña para un objeto.
- ♦ Cambiar la contraseña existente de un objeto.

La definición/cambio de contraseña de NDS está habilitada por defecto. Cuando se inhabilita la clave para definir o cambiar, no podrá definir una nueva contraseña ni cambiar la contraseña existente en eDirectory. Puede habilitar o inhabilitar la definición/cambio de contraseña de NDS en los niveles de la partición y del objeto. Si está inhabilitada la entrada o verificación, no será posible definir ni cambiar las contraseñas.

Antes se podía configurar o cambiar las contraseñas de NDS solo a través de LDAP. Ahora puede hacerlo también a través de iManager. Para obtener más información, consulte la “[Gestión de configuraciones de NDS mediante iManager](#)” en la página 53 y la “[Gestión de configuraciones de NDS a través de LDAP](#)” en la página 53.

Gestión de configuraciones de NDS mediante iManager


En esta sección se incluye la información siguiente:

- ♦ “[Cómo habilitar e inhabilitar la configuración de NDS para una partición](#)” en la página 53
- ♦ “[Cómo habilitar o inhabilitar la configuración de NDS para un objeto](#)” en la página 53

Puede activar la [clave de entrada o verificación](#) o la [clave de definición o cambio](#) en la configuración de entrada de NDS.


Cómo habilitar e inhabilitar la configuración de NDS para una partición

Para habilitar la entrada de NDS para clientes anteriores a eDirectory 8.8:

- 1 En iManager, haga clic en el botón de *Funciones y tareas* .
- 2 Seleccione *NMAS > Aplicación de contraseñas universales*.
- 3 En el módulo auxiliar (plug-in) *Aplicación de contraseñas universales*, seleccione *Configuración de NDS para una partición*.
- 4 Siga las instrucciones del asistente de configuración de NDS para una partición para configurar la gestión de entrada y contraseña en un nivel de partición.
El asistente incluye una sección de ayuda.

Cómo habilitar o inhabilitar la configuración de NDS para un objeto

Para habilitar la entrada de NDS para clientes anteriores a eDirectory 8.8:

- 1 En iManager, haga clic en el botón de *Funciones y tareas* .
- 2 Seleccione *NMAS > Aplicación de contraseñas universales*.
- 3 En el asistente, seleccione *configuración de NDS para un objeto*.
- 4 Siga las instrucciones del asistente de configuración de NDS para un objeto para configurar la gestión de entrada y de la contraseña a nivel de objeto.
El asistente incluye una sección de ayuda.

Gestión de configuraciones de NDS a través de LDAP

Importante: Se recomienda encarecidamente utilizar iManager para gestionar las configuraciones de NDS y no LDAP.

Puede gestionar las configuraciones de NDS a través de LDAP mediante un atributo de eDirectory en un objeto o contenedor raíz de la partición. Los atributos son una parte del esquema de eDirectory 8.7.1 o posterior y no se admiten en eDirectory 8.7 o anterior.

El método utilizado por los clientes heredados para configurar las entradas de NDS se denomina gestión de entrada de NDAP y el método utilizado para las configuraciones de contraseña de NDS se denomina gestión de contraseñas NDAP.

Esta sección proporciona información sobre:

- ♦ [“Cómo habilitar e inhabilitar la configuración de NDS para una partición”](#) en la página 54
- ♦ [“Cómo habilitar o inhabilitar la configuración de NDS para un objeto”](#) en la página 54

Cómo habilitar e inhabilitar la configuración de NDS para una partición

Gestión de entrada y verificación de contraseña

Utilice el atributo `ndapPartitionLoginMgmt` de para habilitar o deshabilitar la gestión de entrada y verificación de contraseña de NDS para una partición.

Valor del atributo <code>ndapPartitionLoginMgmt</code>	Descripción
No está presente o no especificado	La gestión de entrada de NDAP está habilitada.
0	La gestión de entrada de NDAP está inhabilitada.
1	La gestión de entrada de NDAP está habilitada.

Definición y cambio de la contraseña de NDS

Utilice el atributo `ndapPartitionPasswordMgmt` para habilitar o inhabilitar la definición y cambio de una contraseña de NDS para una partición.

Valor del atributo <code>ndapPartitionPasswordMgmt</code>	Descripción
No está presente o no especificado	La gestión de contraseña de NDAP está habilitada.
0	La gestión de contraseña de NDAP está inhabilitada.
1	La gestión de contraseña de NDAP está habilitada.

Cómo habilitar o inhabilitar la configuración de NDS para un objeto

Entrada y verificación de contraseña de NDS

Utilice el atributo `ndapLoginMgmt` para habilitar o inhabilitar la entrada y verificación de contraseña de NDS para un objeto.

Valor del atributo <code>ndapLoginMgmt</code>	Descripción
No está presente o no especificado	La gestión de entrada de NDAP depende de la configuración en el nivel de partición.
0	La gestión de entrada de NDAP está inhabilitada si está inhabilitada en el nivel de partición.
1	La gestión de entrada de NDAP está habilitada independientemente de la opción de configuración en el nivel de partición.

Definición y cambio de la contraseña de NDS

Utilice el atributo `ndapPasswordMgmt` para habilitar o inhabilitar la definición y el cambio de una contraseña de NDS para un objeto.

Valor del atributo ndapPasswordMgmt	Descripción
No está presente o no especificado	La gestión de la contraseña de NDAP depende de la configuración en el nivel de partición.
0	La gestión de contraseña de NDAP está inhabilitada si está inhabilitada en el nivel de partición.
1	La gestión de contraseñas de NDAP está habilitada independientemente de la opción de configuración en el nivel de partición.

Nota: Para obtener más información sobre la creación y gestión de directivas de sincronización de prioridad, consulte [“Using LDAP Tools on Linux”](#) (Uso de herramientas de LDAP en Linux) y [“NetIQ Import Conversion Export Utility”](#) (Utilidad de exportación de conversión de importación de NetIQ) de la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

8.4.3 Operaciones de partición

Cuando se divide una partición, la partición secundaria no hereda las configuraciones de NDS. Cuando mezcla particiones, se conservan las configuraciones de NDS de la partición principal en la partición resultante.

8.4.4 Aplicación de contraseñas que distinguen mayúsculas de minúsculas en un árbol mixto

Si existe un árbol con un servidor eDirectory 8.8 o posterior y un servidor de eDirectory 8.7 o anterior, y los dos servidores comparten una partición, inhabilitar la configuración de entrada de NDS en esa partición tendrá resultados poco fiables. El servidor 8.8 forzará la configuración, impidiendo que los clientes heredados accedan al directorio. Sin embargo, el servidor 8.7 no impondrá la configuración, por lo que se puede obtener acceso al directorio a través del servidor de 8.7.

8.5 Información adicional

Consulte lo siguiente para obtener más información acerca de las contraseñas que distinguen entre mayúsculas y minúsculas:

- ♦ Ayuda en línea de iManager
- ♦ La sección [“Deploying Universal Password”](#) (Implementación de una contraseña universal) en la *NetIQ Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guía de administración de NetIQ Password Management 3.3)

9 Compatibilidad con la directiva de contraseñas de Microsoft Windows Server 2008

En versiones anteriores de eDirectory, los usuarios podrían utilizar la directiva de complejidad por defecto de Microsoft o la sintaxis heredada de Novell. Sin embargo, NetIQ eDirectory 8.8 SP8 admite el uso de directivas de contraseñas que se ajusten a los requisitos de complejidad de directivas de contraseña de Microsoft Windows Server 2008, que difieren de los requisitos de la directiva de complejidad anterior de Microsoft. Puede utilizar iManager para crear una directiva con la nueva opción de sintaxis de directivas de contraseña de Microsoft Windows Server 2008 y configurar la directiva según sea necesario para su entorno.

En este capítulo se proporciona la siguiente información:

- ♦ [Sección 9.1, “Creación de directivas de contraseñas de Windows Server 2008”](#), en la página 57
- ♦ [Sección 9.2, “Gestión de directivas de contraseñas de Windows Server 2008”](#), en la página 58
- ♦ [Sección 9.3, “Información adicional”](#), en la página 58

9.1 Creación de directivas de contraseñas de Windows Server 2008

Puede usar iManager para crear directivas de contraseña que utilizan los requisitos de complejidad de Microsoft Windows Server 2008 y asignar usuarios del entorno eDirectory a la nueva directiva. Para obtener información sobre la creación de directivas de contraseña, consulte la [NetIQ Password Management 3.3.2 Administration Guide \(http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html\)](http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html) (Guía de administración de NetIQ Password Management 3.3.2).

Nota

- ♦ Antes de crear una nueva directiva de contraseña mediante la sintaxis de la directiva de contraseñas de Microsoft Server 2008, asegúrese de instalar la versión más reciente del módulo auxiliar (plug-in) de gestión de contraseñas de Novell iManager. Para obtener más información sobre la instalación de módulos auxiliares (plug-in) de iManager, consulte la [NetIQ iManager 2.7 Administration Guide \(https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html\)](https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html) (Guía de administración de NetIQ iManager 2.7).
 - ♦ También debe asegurarse de que tanto la contraseña universal como las reglas avanzadas de contraseña estén habilitadas para la directiva que desea crear o configurar.
-

9.2 Gestión de directivas de contraseñas de Windows Server 2008

Puede gestionar las directivas que utilizan los requisitos de complejidad de directiva de contraseña de Windows Server 2008 con iManager. Para obtener más información, consulte la sección “Managing Passwords by Using Password Policies” (Gestión de contraseñas mediante directivas de contraseñas) en la *Novell Password Management 3.3.2 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxjj0.html) (Guía de administración de Novell Password Management 3.3.2).

9.3 Información adicional

Consulte lo siguiente para obtener más información sobre las directivas de contraseñas en eDirectory:

- ♦ Ayuda en línea de iManager
- ♦ *Novell Password Management 3.3.2 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)
- ♦ *Novell Modular Authentication Services 3.3.4 Administration Guide* (<http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html>) (Guía de administración de Novell Modular Authentication Services 3.3.4).

10 Sincronización de prioridad

Sincronización de prioridad es una nueva función de NetIQ eDirectory 8.8 que complementa el proceso de sincronización actual en eDirectory. A través de Sincronización de prioridad, puede sincronizar los datos críticos modificados, tales como contraseñas, de manera inmediata.

Puede sincronizar sus datos críticos mediante la sincronización de prioridad cuando no puede esperar a la sincronización normal. El proceso de sincronización de prioridad es más rápido que el proceso de sincronización normal. Se admite la sincronización de prioridad solo entre dos o más servidores de eDirectory 8.8 o posterior que alojan la misma partición.

La tabla siguiente muestra las plataformas compatibles con la función de sincronización de prioridad:

Lista de funciones	Linux	Windows
Sincronización de prioridad	✓	✓

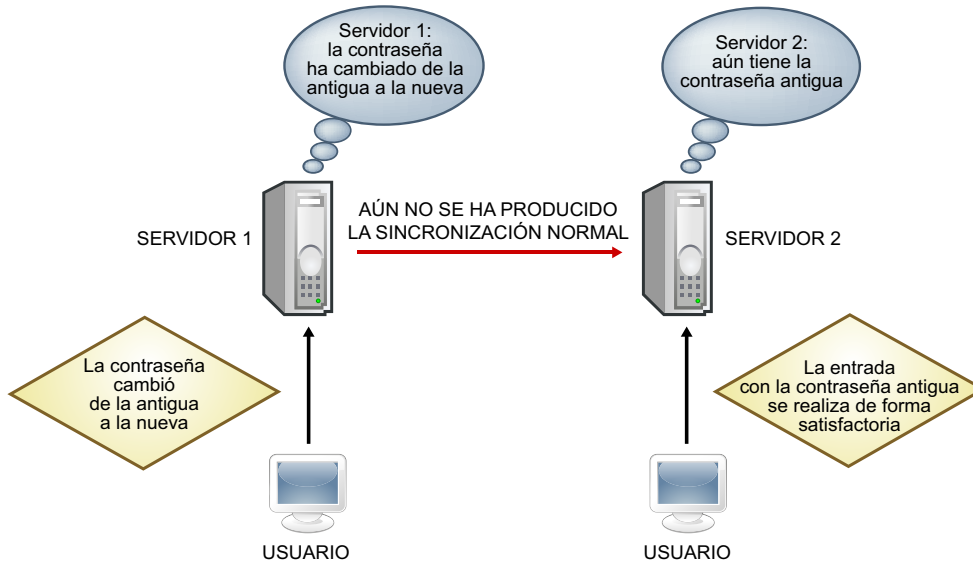
En este capítulo se proporciona la siguiente información:

- ♦ [Sección 10.1, “Necesidad de sincronización de prioridad”, en la página 59](#)
- ♦ [Sección 10.2, “Uso de sincronización de prioridad”, en la página 60](#)
- ♦ [Sección 10.3, “Información adicional”, en la página 60](#)

10.1 Necesidad de sincronización de prioridad

La sincronización normal puede tardar algún tiempo, durante el cual los datos modificados no estarán disponibles en otros servidores. Por ejemplo, supongamos que en la instalación hay diferentes aplicaciones que se comunican con el directorio. Se cambia la contraseña en el servidor 1. Con una sincronización normal, pasa algún tiempo antes de que este cambio se sincroniza con el servidor 2. Por lo tanto, un usuario todavía sería capaz de autenticarse en el directorio a través de una aplicación que se comunique con el servidor 2, utilizando la contraseña antigua.

Figura 10-1 Necesidad de sincronización de prioridad



En implementaciones de gran tamaño, cuando se modifican los datos críticos de un objeto, los cambios han de sincronizarse inmediatamente. El proceso de sincronización de prioridad resuelve este problema.

10.2 Uso de sincronización de prioridad

Para sincronizar las modificaciones de fecha a través de la sincronización de prioridad, debe hacer lo siguiente:

1. Habilitar sincronización de prioridad, configurar el número de hilos y sincronizar mediante prioridad el tamaño de la cola a través de iMonitor.
2. Definir directivas de sincronización de prioridad mediante la identificación de los atributos que son críticos a través de iManager.
3. Aplicar las directivas de prioridad de sincronización a las particiones mediante iManager.

10.3 Información adicional

Consulte los siguientes documentos para obtener más información acerca de la sincronización de prioridad:

- ♦ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).
- ♦ Ayuda en línea de iManager y iMonitor

11 Cifrado de datos

En NetIQ eDirectory 8.8 y versiones posteriores, puede cifrar datos específicos cuando se almacenan en el disco y cuando se transmiten entre dos o más servidores de eDirectory 8.8. Esto proporciona mayor seguridad para los datos confidenciales.

La tabla siguiente muestra las plataformas compatibles con la función de cifrado de datos:

Función	Linux	Windows
Atributos cifrados	✓	✓
Réplica cifrada	✓	✓

En este capítulo se proporciona la siguiente información:

- ♦ [Sección 11.1, “Atributos de cifrado”, en la página 61](#)
- ♦ [Sección 11.2, “Cifrado de replicación”, en la página 62](#)
- ♦ [Sección 11.3, “Información adicional”, en la página 63](#)

11.1 Atributos de cifrado

eDirectory 8.8 permite cifrar los datos confidenciales almacenados en el disco. Atributos cifrados es una función específica del servidor.

Puede tener acceso a atributos cifrados solo a través de canales seguros a menos que decida ofrecer acceso también a través de canales de texto sin cifrar. Consulte [Sección 11.1.3, “Acceda a los atributos cifrados”, en la página 62](#) para obtener más información.

En esta sección se incluye la información siguiente:

- ♦ [Sección 11.1.1, “Necesidad de atributos cifrados”, en la página 61](#)
- ♦ [Sección 11.1.2, “Cómo cifrar los atributos”, en la página 62](#)
- ♦ [Sección 11.1.3, “Acceda a los atributos cifrados”, en la página 62](#)

La característica de cifrado de atributos sólo se admite en eDirectory 8.8 y servidores posteriores.

11.1.1 Necesidad de atributos cifrados

Antes de eDirectory 8.8, los datos se almacenaban en texto no cifrado en el disco. Existía la necesidad de proteger los datos y proporcionar acceso a los datos sólo a través de canales seguros.

Puede utilizar esta función en escenarios donde se necesita proteger datos confidenciales como números de tarjeta de crédito de los clientes del banco.

11.1.2 Cómo cifrar los atributos

Puede cifrar los atributos creando y definiendo directivas de atributos cifrados y, a continuación, aplicar estas directivas a los servidores. Puede crear, definir, aplicar y gestionar directivas de atributos cifrados mediante iManager y LDAP.

- 1 Cree y defina una directiva de atributo de cifrado:
 - 1a Determine los atributos que se van a cifrar.
 - 1b Determine el esquema de cifrado de los atributos.
- 2 Aplique la directiva de atributos cifrados en un servidor.

11.1.3 Acceda a los atributos cifrados

Puede tener acceso a los atributos cifrados solo a través de canales seguros como el puerto SSL LDAP o el puerto HTTP seguro. Si lo desea, puede proporcionar acceso a los atributos cifrados a través de los canales de texto sin cifrar mediante el plug-in de iManager. Para obtener más información, consulte la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

11.2 Cifrado de replicación

Réplica cifrada se refiere al cifrado de datos que se transmiten entre dos o más servidores de eDirectory 8.8.

La réplica cifrada es complementaria a la sincronización normal en eDirectory.

En esta sección se incluye la información siguiente:

- ♦ [Sección 11.2.1, “Necesidad de réplica cifrada”, en la página 62](#)
- ♦ [Sección 11.2.2, “Cómo habilitar la réplica cifrada”, en la página 63](#)

11.2.1 Necesidad de réplica cifrada

Antes de eDirectory 8.8, los datos se transmiten a través del cable durante la replicación en texto sin cifrar. Había la necesidad de proteger los datos confidenciales por la red mediante el cifrado, especialmente si las réplicas estaban separadas geográficamente y conectadas a través de Internet.

Esta función puede utilizarse en los siguientes escenarios:

- ♦ Si los servidores de directorios están repartidos entre ubicaciones geográficas mediante WAN e Internet y existe la necesidad de cifrar datos confidenciales en el cable.
- ♦ Si desea proteger solo algunas particiones del árbol, puede indicar de forma selectiva que se cifren las particiones que alojan los datos confidenciales para llevar a cabo la replicación.
- ♦ Si necesita una réplica cifrada entre réplicas específicas de una partición que contiene datos confidenciales.
- ♦ Si cree que la red de su instalación es hostil, sería conveniente proteger datos confidenciales durante la replicación.

11.2.2 Cómo habilitar la réplica cifrada

Puede habilitar la réplica cifrada mediante iManager. Puede habilitar la réplica cifrada a nivel de partición y de réplica.

Importante: Antes de habilitar la réplica cifrada, asegúrese de que tanto los servidores de origen como de destino tengan los certificados por defecto. Si ha realizado cambios en los certificados, como cambiar de nombre, se produce un error en la replicación cifrada.

11.3 Información adicional

Consulte lo siguiente para obtener más información acerca del cifrado de datos en eDirectory:

- ♦ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).
- ♦ Ayuda en línea de iManager y iMonitor

12 Rendimiento de carga general

NetIQ eDirectory 8.8 proporciona mejoras para aumentar el rendimiento de carga general.

Para obtener más información sobre cómo aumentar la carga general, consulte las siguientes secciones de *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8):

- ♦ [“eDirectory Cache Settings”](#) (Configuración de caché de eDirectory)
- ♦ [“LBURP Transaction Size Setting”](#) (Configuración de tamaño de transacciones LBURP)
- ♦ [“Increasing the Number of Asynchronous Requests in ICE”](#) (Aumento del número de solicitudes asincrónicas in ICE)
- ♦ [“Increased Number of LDAP Writer Threads”](#) (Aumento del número de hilos de escritor de LDAP)
- ♦ [“Disabling Schema Validation in ICE”](#) (Inhabilitar la validación de esquemas en ICE)
- ♦ [“Disabling ACL Templates”](#) (Inhabilitar las plantillas ACL)
- ♦ [“Backlinker”](#)
- ♦ [“Enabling/Disabling Inline Cache”](#) (Habilitar/Inhabilitar el caché en línea)
- ♦ [“Increasing the LBURP Time Out Period”](#) (Aumentar el período límite de LBURP)
- ♦ [“Utilidad de carga general sin conexión”](#)

13 Módulos auxiliares (plug-in) ICE de iManager

Antes de NetIQ eDirectory 8.8, algunas de las opciones de línea de comandos de utilidad de exportación de conversión de importación de Novell (ICE) no tenían las opciones correspondientes en el plug-in de iManager.

En la tabla siguiente se indican las plataformas que admiten esta función:

Función	Linux	Windows
Mejoras de ICE de iManager	✓	✓

El Asistente de ICE en iManager 2.7 con eDirectory 8.8 proporciona las siguientes funciones:

- ♦ [Agregar esquema que falta](#)
- ♦ [Comparar esquema](#)
- ♦ [Generar un archivo de orden](#)

13.1 Agregar esquema que falta

En eDirectory 8.8, iManager proporciona opciones para agregar el esquema que falta al esquema de un servidor. Este proceso implica comparar un origen y un destino. Si hay un esquema adicional en el esquema de origen, se agrega al esquema de destino. El origen puede ser un archivo o un servidor LDAP y el destino debe ser un servidor LDAP.

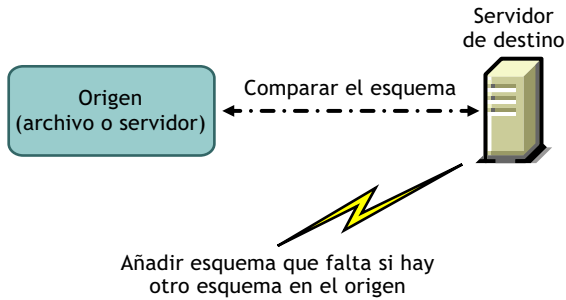
Mediante el asistente de ICE en iManager, puede agregar el esquema que falta mediante las siguientes opciones:

- ♦ [Agregar el esquema desde un archivo](#)
- ♦ [Agregar el esquema desde un servidor](#)

13.1.1 Agregar el esquema desde un archivo

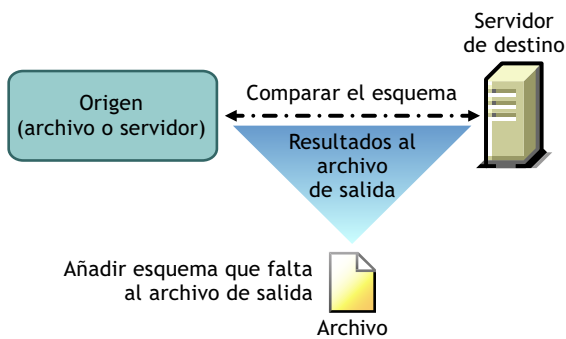
ICE puede comparar el esquema de origen y de destino. El origen es un archivo o un servidor LDAP, y el destino es un servidor LDAP. El archivo de esquema de origen puede ser en formato LDIF o SCH.

Figura 13-1 Comparar y agregar el esquema desde un archivo



Si desea comparar solo el esquema y no agregar el esquema adicional al servidor de destino, seleccione la opción *No añadir el esquema, compararlo*. En este caso, no se agrega el esquema adicional al servidor de destino, pero las diferencias entre el esquema están disponibles como un enlace al final de la operación.

Figura 13-2 Comparar esquemas y agregar los resultados a un archivo de salida



Para obtener más información, consulte [“NetIQ eDirectory Management Utilities”](#) (Utilidades de gestión de NetIQ eDirectory) en la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

13.1.2 Agregar el esquema desde un servidor

El origen y el destino son servidores LDAP.

Si desea comparar solo el esquema y no agregar el esquema adicional al servidor de destino, seleccione la opción *No añadir el esquema, compararlo*. En este caso, no se agrega el esquema adicional al servidor de destino, pero las diferencias entre el esquema están disponibles como un enlace al final de la operación.

Para obtener más información, consulte [“NetIQ eDirectory Management Utilities”](#) (Utilidades de gestión de NetIQ eDirectory) en la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

13.2 Comparar el esquema

Con iManager, puede comparar el esquema entre el origen y el destino. El origen puede ser un archivo o un servidor, y el destino debe ser un archivo LDIF.

iManager compara el esquema entre un origen y un destino y, a continuación, almacena los resultados en un archivo de salida.

Mediante el asistente de ICE de iManager, puede comparar el esquema mediante las siguientes opciones:

- ♦ [Comparar archivos de esquema](#)
- ♦ [Comparar esquema entre un servidor y un archivo](#)

13.2.1 Comparar archivos de esquema

La opción *Comparar archivos de esquema* compara el esquema entre un archivo de origen y un archivo de destino y, a continuación, coloca el resultado en un archivo de salida. Para agregar el esquema que falta en el archivo de destino, aplique los registros del archivo de salida al archivo de destino.

Para obtener más información, consulte “[NetIQ eDirectory Management Utilities](#)” (Utilidades de gestión de NetIQ eDirectory) en la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

13.2.2 Comparar esquema entre un servidor y un archivo

La opción *Comparar esquema entre el servidor y el archivo* compara el esquema entre un servidor de origen y un archivo de destino y, a continuación, coloca el resultado en un archivo de salida. Para agregar el esquema que falta en el archivo de destino, aplique los registros del archivo de salida al archivo de destino.

Para obtener más información, consulte “[NetIQ eDirectory Management Utilities](#)” (Utilidades de gestión de NetIQ eDirectory) en la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

13.3 Generar un archivo de orden

Esta opción crea un archivo de orden que se utilizará con el gestor del delimitador para importar datos de un archivo de datos delimitado. El asistente ayuda a crear este archivo de orden que contiene una lista con los atributos de una clase de objeto específica.

Para obtener más información, consulte “[NetIQ eDirectory Management Utilities](#)” (Utilidades de gestión de NetIQ eDirectory) en la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

13.4 Información adicional

Para obtener más información acerca de esta función, consulte lo siguiente:

- ♦ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).
- ♦ Ayuda en línea de iMonitor

14 Copia de seguridad basada en LDAP

En NetIQ eDirectory 8.8 se incluye la función de copia de seguridad basada en LDAP. Esta función se utiliza para hacer una copia de seguridad de los atributos y sus valores para cada objeto.

En la tabla siguiente se indican las plataformas que admiten esta función:

Función	Linux	Windows
Copia de seguridad basada en LDAP	✓	✓

Esta función le permite realizar una copia de seguridad incremental en la que solo se hace una copia de seguridad si hay cambios en el objeto.

La copia de seguridad basada en LDAP proporciona un conjunto de interfaces para copia de seguridad y restauración de objetos de eDirectory expuestos a través de las bibliotecas de LDAP para C a través de operaciones extendidas de LDAP.

Para obtener más información sobre SDK de bibliotecas de LDAP para de C, consulte la [Bibliotecas de LDAP para la documentación de C \(http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html\)](http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

Para obtener un ejemplo de cómo hacer una copia de seguridad y restauración de objetos de eDirectory a través de LDAP, consulte el código de ejemplo backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

14.1 Necesidad de copia de seguridad basada en LDAP

La copia de seguridad basada en LDAP intenta resolver los problemas existentes con la copia de seguridad y restauración actual.

Los problemas que resuelve esta función son:

- ♦ Proporciona una interfaz coherente con la que cualquier aplicación de copia de seguridad de terceros o desarrollador pueden hacer copia de seguridad de eDirectory en todas las plataformas compatibles.
- ♦ Proporciona una solución de copia de seguridad para copiar objetos de manera incremental.

14.2 Información adicional

Para obtener más información acerca de esta función, consulte lo siguiente:

- ♦ Bibliotecas LDAP para C (<http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html>).
- ♦ Código de ejemplo: `backup.c` (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html).

15 Obtener lista de privilegios eficaces de LDAP

La API para obtener la lista de privilegios eficaces LDAP se introdujo con NetIQ eDirectory 8.8 SP6.

En la tabla siguiente se indican las plataformas que admiten esta función:

Función	Linux	Windows
Obtener lista de privilegios eficaces de LDAP	✓	✓

Esta función puede utilizarse para obtener los privilegios efectivos de un DN de tema en particular en un DN de destino dado para un determinado conjunto de atributos. Esto proporciona una interfaz para obtener la lista de privilegios a través de las bibliotecas LDAP para C mediante operaciones extendidas de LDAP.

Para obtener más información sobre SDK de bibliotecas de LDAP para C, consulte la documentación sobre [Bibliotecas de LDAP para C \(http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html\)](http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

15.1 Necesidad de interfaz para obtener lista de privilegios eficaces de LDAP

La interfaz para obtener la lista de privilegios eficaces de LDAP intenta resolver los problemas que presenta la API para obtener privilegios eficaces.

Los problemas que resuelve esta función son:

- ♦ Requiere una sola única solicitud al directorio para obtener los derechos efectivos para múltiples atributos.
- ♦ Reduce el tiempo de ida y vuelta al directorio para obtener los derechos efectivos para múltiples atributos.
- ♦ Identifica los errores en las entradas en la solicitud o en el directorio.

15.2 Información adicional

Para obtener más información acerca de esta función, consulte lo siguiente:

- ♦ [Bibliotecas LDAP para C \(http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html\)](http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html).
- ♦ Código de ejemplo: [getpriv.c \(http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html\)](http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html).

16 Gestión del registro de errores en eDirectory 8.8

Muchos clientes han informado de que el registro de errores en NetIQ eDirectory no sirve de mucho en la identificación y resolución de los problemas comunes. El registro de errores se inicia automáticamente durante la instalación de eDirectory.

Este capítulo consta de las siguientes secciones:

- ♦ [Sección 16.1, “Niveles de gravedad del mensaje”, en la página 75](#)
- ♦ [Sección 16.2, “Configuración del registro de errores”, en la página 76](#)
- ♦ [Sección 16.3, “Mensajes de DTrace”, en la página 79](#)
- ♦ [Sección 16.4, “Filtrado de mensajes de iMonitor”, en la página 82](#)
- ♦ [Sección 16.5, “Filtrado de mensajes de SAL”, en la página 82](#)

16.1 Niveles de gravedad del mensaje

Todos los mensajes tienen un nivel de gravedad asociado que le ayudará a determinar la importancia del mensaje. Los niveles en orden descendente de gravedad son:

- ♦ [Sección 16.1.1, “Fatal”, en la página 75](#)
- ♦ [Sección 16.1.2, “Advertencia”, en la página 75](#)
- ♦ [Sección 16.1.3, “Error”, en la página 76](#)
- ♦ [Sección 16.1.4, “Información”, en la página 76](#)
- ♦ [Sección 16.1.5, “Depurar”, en la página 76](#)

16.1.1 Fatal

Un mensaje clasificado como fatal indica un problema importante, como la pérdida de datos o de funcionalidad.

Ejemplos:

- ♦ Si se produce un error en el servidor eDirectory al cargar los módulos del sistema como NCP Engine y DSLoader, se comunica un error fatal y queda registrado.
- ♦ Si se produce un error en el servidor eDirectory al asociarse al puerto seguro 636, se comunica un error y queda registrado.

16.1.2 Advertencia

Un mensaje que no es necesariamente grave, pero podría ser una posible causa de problemas en el futuro.

Ejemplos:

- ♦ Errores de conexión entre dos servidores del árbol, lo que hace que el servidor se añada a un caché de dirección no válida. El servidor puede recuperarse de este estado en particular restableciendo el caché de la dirección no válida.
- ♦ Si la aplicación de cliente LDAP establece una asociación y cierra la conexión sin desasociarla, entonces el servidor LDAP debe registrar una advertencia con el mensaje de advertencia correspondiente.
- ♦ Si el servidor eDirectory ha agotado todos los descriptores de archivo y se ha alcanzado el límite de umbral, el servidor no será capaz de procesar las solicitudes entrantes y responder a ellas, lo que conducirá a un error de la aplicación.

16.1.3 Error

Un mensaje que podría tener origen en una operación no válida, pero que no causará ningún problema.

Ejemplos:

- ♦ Cuando una aplicación de cliente intenta agregar un objeto cuyos atributos no están definidos en el esquema, el servidor eDirectory notificará el error ERR_NO_SUCH_ATTRIBUTE.
- ♦ Cuando un usuario intenta entrar con una contraseña no válida, el servidor eDirectory notificará el error ERR_FAILED_AUTHENTICATION.

16.1.4 Información

Un mensaje que describe la correcta finalización de una operación o un evento en el servidor eDirectory.

Ejemplos:

- ♦ Cuando un módulo se carga o descarga correctamente, puede ser adecuado registrar un mensaje informativo de la operación.
- ♦ Cuando cambia la configuración del caché de base de datos, deben registrarse mensajes informativos al guardar correctamente la configuración.

16.1.5 Depurar

Un mensaje que contiene información que ayudará a los desarrolladores en la depuración de un programa.

Ejemplos:

Al realizar una búsqueda de grupo dinámico, muestre todos los miembros del grupo dinámico con la información de entrada, ID, ID de partición y el DN de todos los miembros. Esta información ayudará a saber que todos los miembros regresan al nivel de eDirectory.

16.2 Configuración del registro de errores

- ♦ [Sección 16.2.1, "Linux", en la página 77](#)
- ♦ [Sección 16.2.2, "Windows", en la página 77](#)

16.2.1 Linux

Para configurar los ajustes del registro de errores de los mensajes en el lado del servidor, puede utilizar los parámetros `n4u.server.log-levels` y `n4u.server.log-file` del archivo de configuración `/etc/opt/novell/eDirectory/conf/nds.conf`.

Definición del nivel de gravedad

Los niveles de gravedad disponibles son `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` y `LogDbg` (en orden descendente de gravedad). Para obtener más información sobre los niveles de gravedad, consulte la [Sección 16.1, “Niveles de gravedad del mensaje”, en la página 75](#).

Por defecto, el nivel de gravedad se establece en `LogFatal`. Por lo tanto, sólo se registrarán los mensajes con nivel de gravedad Fatal.

Para establecer el nivel de gravedad, utilice el parámetro `n4u.server.log-levels` del archivo `nds.conf` de la siguiente manera:

```
n4u.server.log-levels=severity_level
```

Por ejemplo:

- ♦ Para establecer el nivel de gravedad en `LogInfo` y superiores, escriba lo siguiente:

```
n4u.server.log-levels=LogInfo
```

Con esta configuración, los mensajes con nivel de gravedad `LogInfo` y superiores (es decir, `LogFatal` `LogWarn` `LogErr`) se registrarán en el archivo de registro.

- ♦ Para establecer el nivel de gravedad en `LogWarn` y superiores, escriba lo siguiente:

```
n4u.server.log-levels=LogWarn
```

Con esta configuración, los mensajes con nivel de gravedad `LogWarn` y superiores (`LogFatal`) se registrarán en el archivo de registro.

Cómo especificar el nombre del archivo de registro

Para especificar la ubicación del archivo de registro donde se registrarán los mensajes, utilice el parámetro `n4u.server.log-file` en el archivo `nds.conf`. Por defecto, los mensajes se registran en el archivo `ndsd.log`.

Por ejemplo, para registrar los mensajes en `/tmp/edir.log`, escriba lo siguiente:

```
n4u.server.log-file=/tmp/edir.log
```

Para registrar los mensajes en el registro del sistema, utilice el parámetro `n4u.server.log-file` de la manera siguiente:

```
n4u.server.log-file=syslog
```

16.2.2 Windows

- ♦ [“Definición del nivel de gravedad” en la página 78](#)
- ♦ [“Cómo especificar el nombre y la vía al archivo de registro” en la página 78](#)
- ♦ [“Cómo especificar el tamaño del archivo de registro” en la página 78](#)

Definición del nivel de gravedad

Los niveles de gravedad disponibles son LogFatal, LogWarn, LogErr, LogInfo y LogDbg (en orden descendente de gravedad). Para obtener más información sobre los niveles de gravedad, consulte la [Sección 16.1, “Niveles de gravedad del mensaje”, en la página 75](#).

Para establecer el nivel de gravedad, haga lo siguiente:

- 1 Haga clic en *Inicio > Configuración > Panel de control > NetIQ eDirectory Services*
- 2 En la pestaña *Servicios*, seleccione *dhlog.dlm*.
- 3 Especifique el nivel de registro en el cuadro *Parámetros de inicio*.

Por ejemplo, para establecer el nivel de registro en LogErr y superiores, escriba lo siguiente:

```
LogLevel=LogErr
```

- 4 Haga clic en *Configurar*
- 5 En la pestaña *Configuración de ACS*, haga clic en el signo más de *DHostLogger*.
El parámetro LogLevel se actualiza con el valor configurado.

Cómo especificar el nombre y la vía al archivo de registro

- 1 Haga clic en *Inicio > Configuración > Panel de control > NetIQ eDirectory Services*
- 2 En la pestaña *Servicios*, seleccione *dhlog.dlm*.
- 3 Escriba la vía al archivo de registro en *Parámetros de inicio* de la forma siguiente:

```
LogFile=file_path
```

Por ejemplo, para establecer la vía al archivo de registro en /tmp/Err.log , escriba lo siguiente en parámetros de inicio:

```
LogFile=/tmp/Err.log
```

- 4 Haga clic en *Configurar*
- 5 En la pestaña *Configuración de ACS*, haga clic en el signo más de *DHostLogger*.
El parámetro LogFile se actualiza con el valor configurado.

Cómo especificar el tamaño del archivo de registro

- 1 Haga clic en *Inicio > Configuración > Panel de control > NetIQ eDirectory Services*
- 2 En la pestaña *Servicios*, seleccione *dhlog.dlm*.
- 3 Escriba la vía al archivo de registro *Parámetros de inicio* de la forma siguiente:

```
LogSize=size
```

El tamaño por defecto es 1 MB.

- 4 Haga clic en *Configurar*
- 5 En la pestaña *Configuración de ACS*, haga clic en el signo más de *DHostLogger*.
El parámetro LogSize se actualiza con el valor configurado.

16.3 Mensajes de DSTrace

Puede filtrar los mensajes de seguimiento en función de la ID de hilo, la ID de conexión y gravedad de los mensajes.

Después de especificar un filtro para los mensajes, solo los mensajes que coinciden con el filtro se muestran en la pantalla. Todos los demás mensajes de las etiquetas habilitadas se registrarán en el archivo `ndstrace.log` si este se ha configurado en ACTIVADO.

Solo se aplica un filtro a la vez. Debe especificarse un filtro para cada sesión de DSTrace.

Por defecto, se establece el nivel de gravedad en INFO, lo que significa que se mostrarán todos los mensajes con nivel de gravedad superiores a INFO. Puede ver el nivel de gravedad habilitando la etiqueta `svty`.

También puede usar iMonitor para filtrar los mensajes de seguimiento. Para obtener más información, consulte la [Sección 16.4, "Filtrado de mensajes de iMonitor"](#), en la página 82.

16.3.1 Linux

Complete el siguiente procedimiento para filtrar los mensajes de seguimiento:

- 1 Habilite el filtrado con el siguiente comando:

```
ndstrace tag filter_value
```

Para inhabilitar el filtrado, escriba el siguiente comando:

```
ndstrace tag
```

Ejemplos para habilitar el filtrado:

- ♦ Para habilitar el filtrado para la ID de hilo 35, escriba lo siguiente:

```
ndstrace thrd 35
```

- ♦ Para habilitar el filtrado para el nivel de gravedad fatal, escriba lo siguiente:

```
ndstrace svty fatal
```

Los niveles de gravedad pueden ser FATAL, ADVERTENCIA, ERROR, INFO y DEPURAR.

- ♦ Para habilitar el filtrado para la ID de conexión 21, escriba lo siguiente:

```
ndstrace conn 21
```

Ejemplos para inhabilitar el filtrado:

- ♦ Para inhabilitar el filtrado basado en la ID de hilo, escriba lo siguiente:

```
ndstrace thrd
```

- ♦ Para inhabilitar el filtrado basado en la ID de conexión, escriba lo siguiente:

```
ndstrace conn
```

- ♦ Para inhabilitar el filtrado basado en la gravedad, escriba lo siguiente:

```
ndstrace svty
```

Figura 16-1 Ejemplo de pantalla de mensaje de seguimiento con filtros

```
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 241, size 121, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 120, size 32, err 0.
NCPEng : INFO : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 120, size 54, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 121, size 248, err 0.
NCPEng : INFO : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent : DEBUG : Calling DSAResolveName conn:22 for client .[Public].
Reslv : DEBUG : ConvertDNToID: dn=\T=WIN-0510\0=novell\CN=OSG-NTS-2-MDS, cts=4281a5dc:01:001
NCPCLI : DEBUG : DCCreateContext context 3464002c moduleHandle 60000000 C:\Novell\NDS\ds.dlm, idHandle 00000000
Reslv : DEBUG : Connect to tcp:164.99.148.219:524 succeeded
DRL : INFO : Primary object is ID_INVALID
NCPCLI : DEBUG : DCFreeContext context 3464002c idHandle 00000000, connHandle 00001b00, C:\Novell\NDS\ds.dlm
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 121, size 74, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 242, size 32, err 0.
NCPEng : INFO : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 242, size 46, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 243, size 196, err 0.
NCPEng : INFO : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent : DEBUG : Calling DSASstartUpdateReplica conn:14 for client .OSG-NTS-2-MDS.novell.WIN-0510.
Reslv : DEBUG : ConvertDNToID: dn=\T=WIN-0510, cts=4281a5dc:01:001
SyncI : INFO : ** SYNCHRONIZATION DISABLED! .WIN-0510., .OSG-NTS-2-MDS.novell.WIN-0510.
Agent : DEBUG : DSASstartUpdateReplica failed, synchronization disabled (-701).
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 243, size 32, flags 0, ncperr 0.
```

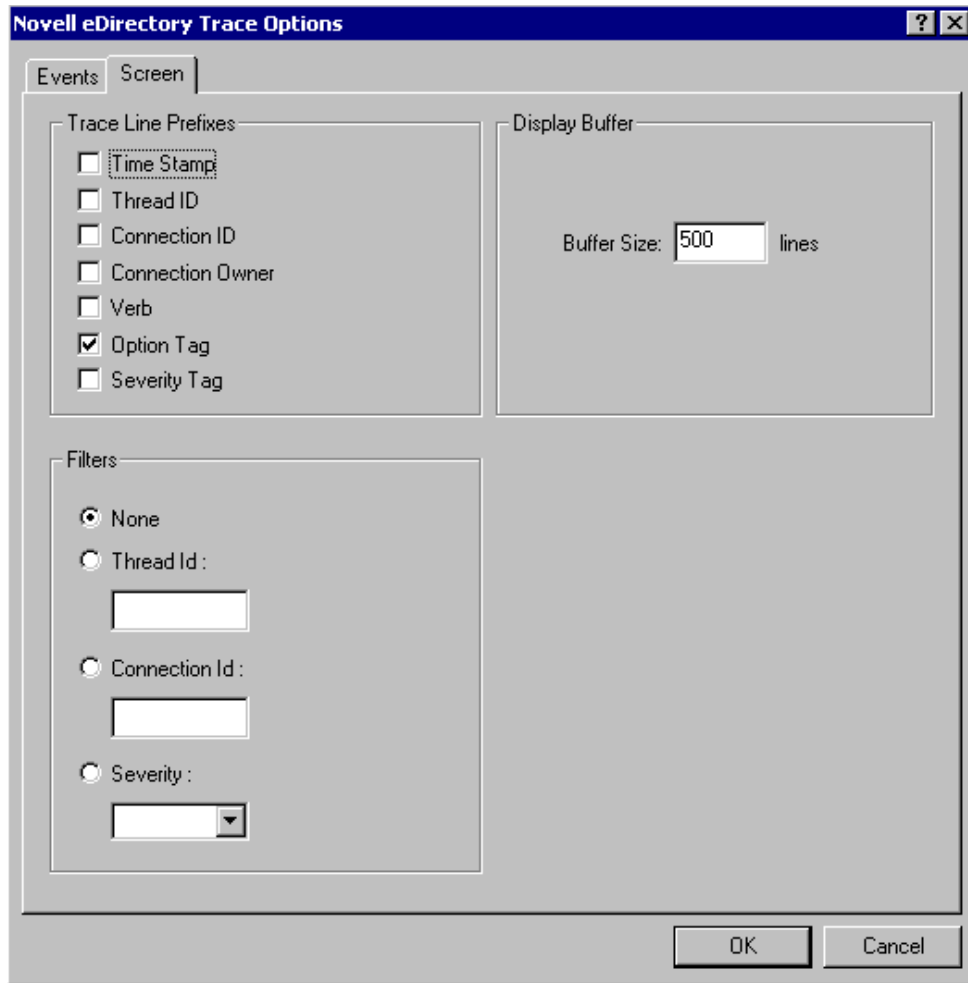
16.3.2 Windows

Complete el siguiente procedimiento para filtrar los mensajes de seguimiento:

- 1 Seleccione *Inicio > Panel de Control > NetIQ eDirectory Services*
- 2 En la pestaña *Servicios*, seleccione *dstrace.dlm*.
- 3 Haga clic en *Editar > Opciones* en la ventana de seguimiento.

Se muestra el cuadro de diálogo de Opciones de seguimiento de NetIQ eDirectory.

Figura 16-2 Pantalla de opciones de seguimiento en Windows



4 Haga clic en la pestaña *Pantalla*.

5 Seleccione la opción de filtro en el grupo de *Filtros* e introduzca el valor del filtro.

Puede filtrar los mensajes en función en:

- ◆ ID de hilo
- ◆ ID de conexión
- ◆ Gravedad

Antes de seleccionar cualquiera de los filtros, asegúrese de que esté habilitado en *Prefijos de línea de seguimiento*.

También puede inhabilitar el filtrado seleccionando *Ninguno* o desactivando la opción de filtro.

Nota: Si ha seleccionado *ID de hilo* o *ID de conexión* como la opción de filtro y especifica un valor que no existe, no se mostrarán los mensajes en la pantalla. Sin embargo, todavía se registrarán todos los demás mensajes en el archivo `ndstrace.log`.

16.4 Filtrado de mensajes de iMonitor

Puede filtrar los mensajes de seguimiento iMonitor en función de la ID de conexión, la ID de hilo o el número de error.

Para filtrar en función de la ID de conexión y la ID de hilo, asegúrese de que las habilitado en la pestaña Configuración de seguimiento.

Para obtener más información, consulte la ayuda en línea de iMonitor.

16.5 Filtrado de mensajes de SAL

SAL se ha mejorado para registrar información detallada sobre errores a pedido. Puede hacerse un seguimiento de las llamadas de función con argumentos en las versiones de depuración.

16.5.1 Configuración de los niveles de gravedad

Puede usar el parámetro `SAL_LogLevels` para configurar los niveles de seguridad para los mensajes SAL. `SAL_LogLevels` es una lista separada por comas de los niveles de registro deseados.

En la siguiente tabla se explican los niveles de registro:

Tabla 16-1 *Parámetros de filtrado de mensajes SAL*

Nombre del parámetro	Descripción
LogCrit	Mensajes críticos. Este nivel está habilitado por defecto. Después de registrarse un error crítico, apague el sistema.
LogErr	Todos los mensajes de error. El sistema sigue funcionando, pero los resultados son imprevisibles.
LogWarn	Mensajes de advertencia. Esto es sólo una advertencia para que tenga conocimiento de algún error inminente.
LogInfo	Mensajes informativos.
LogDbg	Mensajes de depuración que se utilizan para la depuración en el momento de desarrollo. Estos mensajes se compilan desde una versión de lanzamiento para reducir el tamaño de código binario.
LogCall	Realiza un seguimiento de las llamadas de función. Se trata de un subconjunto de los mensajes de depuración.
LogAll	Habilita todos los mensajes excepto LogCall.

Un "-" al principio de un determinado nivel de registro específico inhabilita ese nivel.

Ejemplos

Para filtrar basándose en todos los niveles de registro, excepto LogInfo y LogDbg, realice los pasos siguientes:

Linux

- 1 Detenga ndsd.
- 2 Escriba el comando siguiente:

```
export SAL_LogLevels=LogAll, -LogInfo, -LogDbg
```

- 3 Inicie ndsd.

Windows

- 1 Apague DHost.
- 2 Escriba el siguiente comando en la línea de comandos:

```
set SAL_LogLevels=LogAll, -LogInfo, -LogDbg  
c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
```

- 3 Reinicie DHost.

16.5.2 Definición de la vía al archivo de registro

Puede utilizar la variable de entorno de SAL_LogFile para especificar la ubicación del archivo de registro. Esto puede ser un nombre de archivo válido con una vía válida o una de las siguientes.

- ♦ Consola: se registran todos los mensajes en la consola.
- ♦ Syslog: en Linux, los mensajes pasan en el registro del sistema. En Windows, los mensajes se registran en un archivo con el nombre syslog. Este es el comportamiento por defecto para el registro.

Todos los errores críticos se registran siempre en syslog, salvo que esté específicamente inhabilitado.

17 Utilidad de carga general sin conexión: Ldif2dib

Ldif2dib es una nueva utilidad introducida en NetIQ eDirectory 8.8 para la carga general de datos desde archivos LDIF a la base de datos de eDirectory. Se trata de una utilidad sin conexión y logra cargas generales más rápidas en comparación con las demás herramientas en línea.

En la tabla siguiente se indican las plataformas que admiten Ldif2dib.

Función	Linux	Windows
Ldif2dib	✓	✓

17.1 Necesidad de Ldif2dib

Se necesita la utilidad Ldif2dib cuando una base de datos de usuarios de gran dimensión debe llenarse con las entradas de un archivo LDIF. Las herramientas en línea como ice o ldapmodify son más lentas que Ldif2dib en este sentido, debido a la sobrecarga asociada a la carga general en línea, como la comprobación de esquemas, traducción de protocolo y comprobaciones de control de acceso. Ldif2dib permite un tiempo de actividad rápido cuando se necesita completar una base de datos de usuarios de gran dimensión y cuando el tiempo de inactividad inicial no es un problema.

17.2 Información adicional

Para obtener más información sobre esta utilidad, consulte [“Offline Bulkload Utility”](#) (Utilidad de carga general sin conexión) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).

18 Copia de seguridad de eDirectory con SMS

Servicios de gestión de almacenamiento de Novell (SMS) es un marco de API utilizado por aplicaciones de copia de seguridad para proporcionar una solución de copia de seguridad completa. El marco de trabajo SMS se implementa mediante dos componentes principales:

- ♦ Requester de datos de gestión de almacenamiento (SMDR)
- ♦ Agente de servicios de destino (TSA)

El TSA para los servicios de eDirectory (`tsands`) está destinado y proporciona una implementación de la API de servicios de gestión de almacenamiento de Novell a los árboles de directorios. Las aplicaciones se pueden escribir sobre la API de SMS para proporcionar una solución de copia de seguridad completa.

El TSA de NDS es compatible con Linux.

19 Auditoría de LDAP

La auditoría es una de las principales funcionalidades que interesan a los administradores al evaluar un directorio. El mecanismo de eventos eDirectory facilita la auditoría de eDirectory. Dado que las aplicaciones están adoptando en gran medida el protocolo LDAP para tener acceso a los directorios, el requisito de la auditoría de operaciones LDAP es muy extendido.

Este capítulo consta de las siguientes secciones:

- ♦ [Sección 19.1, “Necesidad de auditoría de LDAP”, en la página 89](#)
- ♦ [Sección 19.2, “Uso de auditoría LDAP”, en la página 89](#)
- ♦ [Sección 19.3, “Información adicional”, en la página 90](#)

19.1 Necesidad de auditoría de LDAP

Este mecanismo de eventos estaba manifiestamente ausente en el servidor LDAP de eDirectory existente que no podía proporcionar suficiente información sobre LDAP. Aunque el sistema de eventos NDS producía eventos para todas las operaciones de eDirectory, la mayor parte de esta información era insuficiente o irrelevante para que una aplicación auditara el servidor LDAP. La información referente al protocolo y los detalles de asociación, la dirección de red, los métodos de autenticación, los tipos de autenticación, la búsqueda de LDAP y los detalles de la transacción, entre otros, que son vitales para la auditoría de un servidor LDAP, no estaban disponibles con los eventos NDS. A los desarrolladores de aplicaciones les resultaba difícil escribir aplicaciones de auditoría LDAP basadas en estos eventos.

Dado que LDAP es una interfaz importante de eDirectory, para proporcionar un mecanismo para que las aplicaciones realicen una auditoría del servidor LDAP de eDirectory, se ha introducido un subsistema de eventos de LDAP en la versión NetIQ eDirectory 8.8 SP3. Este subsistema genera eventos específicos de LDAP con toda la información relevante para que una aplicación pueda auditar un servidor LDAP. Esto se conoce como auditoría de LDAP.

19.2 Uso de auditoría LDAP

La auditoría de LDAP permite a las aplicaciones supervisar o auditar las operaciones de LDAP tales como agregar, modificar, buscar, etc. y obtiene información útil del servidor LDAP como la información de conexión, la IP del cliente al que se conectó el servidor en el momento de la operación de LDAP, el identificador del mensaje, el código de resultado de la operación y así sucesivamente.

La auditoría de LDAP puede ejercerse a través de la [NDK de bibliotecas de LDAP para C](http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html) (<http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html>), que proporciona la interfaz en el lado del cliente de esta función a través de nuevos eventos y estructuras de LDAP.

19.3 Información adicional

Consulte lo siguiente para obtener más información sobre los eventos de auditoría de LDAP:

- ♦ “[Configuring LDAP Services for NetIQ eDirectory](#)” (Configuración de servicios LDAP para NetIQ eDirectory) en la *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guía de administración de NetIQ eDirectory 8.8 SP8).
- ♦ [NDK: Herramientas de LDAP](http://developer.novell.com/documentation/cldap/ltolenu/data/hevgtl7k.html) (<http://developer.novell.com/documentation/cldap/ltolenu/data/hevgtl7k.html>) en la documentación de bibliotecas de LDAP para C.

Para obtener información sobre herramientas de LDAP, consulte [Bibliotecas de LDAP para C](http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html) (<http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html>).

20 Auditoría con XDASv2

La especificación XDASv2 proporciona una clasificación estandarizada de eventos de auditoría. Define un conjunto de eventos genéricos en el nivel de sistema distribuido global. XDASv2 proporciona un formato de registro de auditoría portátil común que facilita la fusión y el análisis de información de auditoría procedente de diversos componentes en el nivel de sistema distribuido. Los eventos XDASv2 se encapsulan en un sistema notacional jerárquico que ayuda a ampliar el conjunto de identificadores de evento estándar o existente.

Con eDirectory 8.8 SP8, si el agente de XDASv2 no se puede comunicar con el servidor de registro del sistema, el agente puede configurarse para almacenar en caché local los eventos de auditoría registrados, lo que garantiza que no se pierdan datos de auditoría. Después el agente intenta volver a enviar los eventos de auditoría almacenados, continuando hasta que se restablece la comunicación. El almacenamiento en caché de eventos XDAS está inhabilitado por defecto.

Para obtener más información, consulte la [NetIQ XDASv2 Administration Guide](#) (Guía de administración de NetIQ XDASv2).

21 Miscelánea

Este capítulo trata varias funciones nuevas de NetIQ eDirectory 8.8.

- ♦ Sección 21.1, “Generación de informes sobre volcado de caché en iMonitor”, en la página 93
- ♦ Sección 21.2, “Compatibilidad de sintaxis de entero grande de Microsoft en iManager”, en la página 93
- ♦ Sección 21.3, “Almacenamiento en caché del objeto de seguridad”, en la página 94
- ♦ Sección 21.4, “Mejora del rendimiento de la búsqueda de subárbol”, en la página 94
- ♦ Sección 21.5, “Cambios de localhost”, en la página 95
- ♦ Sección 21.6, “Controlador de archivo 256 en Solaris”, en la página 95
- ♦ Sección 21.7, “Administrador de memoria en Solaris”, en la página 95
- ♦ Sección 21.8, “Grupos anidados”, en la página 95

21.1 Generación de informes sobre volcado de caché en iMonitor

La página Caché cambios en iMonitor muestra sólo un objeto a la vez, lo que hace que sea difícil examinar el caché de cambios completo. eDirectory 8.8 SP8 agrega un nuevo informe de volcado de caché de cambios a los informes por defecto que se incluyen con iMonitor. Con este informe, puede ver todo el caché de cambios a la vez. Este informe puede ayudar a un administrador a comprender mejor los cambios que se producen en un servidor determinado.

Al ejecutar un informe de volcado de caché de cambios, iMonitor también genera un volcado XML completo de todos los objetos en el caché, junto con los atributos y valores que se deben sincronizar entre servidores.

Para obtener información sobre los informes iMonitor, consulte la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

21.2 Compatibilidad de sintaxis de entero grande de Microsoft en iManager

eDirectory 8.8 SP8 proporciona una nueva sintaxis compatible con la sintaxis de entero grande de Microsoft. Esta sintaxis puede servir para almacenar valores enteros grandes o fechas anteriores a 1970 o posteriores a 2038. Puede utilizar LDAP o iManager para crear o gestionar atributos con esta sintaxis.

Nota: eDirectory sigue utilizando su sintaxis existentes y valores de 32 bits para las marcas horarias internas.

21.3 Almacenamiento en caché del objeto de seguridad

Cuando el primer servidor se instala en el árbol y contiene información como datos globales, directivas de seguridad y claves, se crea el contenedor de seguridad a partir de la partición raíz.

Después de introducirse la contraseña universal, siempre que un usuario entraba en eDirectory a través de NMAS, NMAS accedía a la información del contenedor de seguridad para autenticar la entrada. Cuando la partición con el contenedor de seguridad no estaba presente a nivel local, NMAS accedía al servidor, que tenía esta partición. Esto tenía un impacto negativo en el rendimiento de la autenticación NMAS. La situación era peor cuando había que acceder al servidor que contiene la partición que alojaba contenedor de seguridad a través de enlaces de WAN.

Para resolver este problema, en eDirectory 8.8, los datos del contenedor de seguridad se almacenan en caché en el servidor local. Por lo tanto, NMAS no necesita acceder al contenedor de seguridad ubicado en un equipo diferente cada vez que un usuario inicia una sesión, ya que se puede acceder fácilmente a nivel local. Esto aumenta el rendimiento. Agregar la partición que tiene el contenedor de seguridad a un servidor local mejora el rendimiento, pero no sería viable en situaciones donde hay demasiados servidores.

Si cambian los datos reales en el contenedor de seguridad en el servidor que contiene la partición del contenedor de seguridad, se actualiza la memoria caché local en un proceso en segundo plano llamado backlinker. Por defecto, backlinker se ejecuta cada trece horas y obtiene los datos modificados del servidor remoto. En caso de que, los datos deban sincronizarse inmediatamente, puede programar backlinker en el servidor local a través de iMonitor, ndstrace en Linux o ndscons en Windows. Para obtener más información, consulte la ayuda en línea de iMonitor o el manual de ndstrace.

La función de almacenamiento en caché de objetos de seguridad está habilitada por defecto. Si no desea que backlinker almacene ningún dato en caché, elimine `CachedAttrsOnExtRef` del objeto de servidor NCP.

21.4 Mejora del rendimiento de la búsqueda de subárbol

El rendimiento de la búsqueda de subárbol de eDirectory para un árbol de gran tamaño con una estructura anidada significativamente permanece plano independientemente del DN base de la búsqueda. Esto se ha resuelto mediante un atributo de `AncestorID`. El atributo `AncestorID` es una lista de identificadores de entrada de todos los antecesores, asociados con cada entrada. Este atributo de `AncestorID` se utiliza internamente durante la búsqueda de subárbol y, por tanto, restringe el ámbito de la búsqueda.

Este atributo se rellena al agregar una entrada y después de la actualización de todas las entradas en el archivo DIB y se vuelve a llenar para todas las entradas del subárbol después mover un subárbol. Sin embargo, la búsqueda de subárbol no utilizará el atributo `AncestorID` mientras llena el atributo después de actualizar y mover el subárbol. Por lo tanto, el rendimiento del subárbol sigue siendo similar al rendimiento de la búsqueda de subárbol anterior a eDirectory 8.8.

Para comprobar si se ha actualizado `AncestorIDs` después de la actualización:

Una vez completado `AncestorIDs`, cambia la versión de actualización de objeto NDS a 6 o más. Puede visualizar esto mediante iMonitor en la sección *Historial de DIB* de Información de agente.

Para comprobar si `AncestorIDs` se actualizan después de la operación de movimiento del subárbol:

Mientras se completan `AncestorIDs`, el atributo `UpdateInProgress` del objeto `Pseudo Server` tiene la lista de ID de entrada de la raíz de partición del subárbol. Una vez completado `AncestorIDs`, el atributo no estará presente en el `Pseudoservidor`.

`DSRepair` actualiza el atributo `AncestorID` si no es válido.

21.5 Cambios de localhost

Los servidores de eDirectory 8.8 no escuchan en la dirección de bucle invertido. Las utilidades que usan localhost deben cambiarse para utilizar el nombre de host o la resolución de direcciones IP.

Si cualquier herramienta o utilidad de terceros se resuelve través de localhost, es necesario cambiarla para que se resuelva a través de un nombre de host o dirección IP, no a través de la dirección de localhost.

21.6 Controlador de archivo 256 en Solaris

Anteriormente, la implementación de transmisiones de Solaris 2.x `stdio` solo podía utilizar un máximo de 256 descriptores de archivo. Esto era insuficiente para que eDirectory funcionara correctamente. eDirectory 8.8 proporciona una biblioteca de seudorutinas auxiliar para superar este límite.

21.7 Administrador de memoria en Solaris

Las versiones anteriores de eDirectory en Solaris utilizaban Geodesic^{*}, un producto de terceros, como el Administrador de memoria. Con esta versión, eDirectory 8.8 no incluye los asignadores de memoria de otros fabricantes, pero utiliza el administrador de memoria nativa.

Esto no influye en el rendimiento de eDirectory. En la mayoría de los casos, el rendimiento ha mejorado o seguía siendo el mismo que el distribuidor de los productos de terceros.

21.8 Grupos anidados

eDirectory 8.8 SP2 admite la agrupación de grupos, lo que proporciona una forma más estructurada de agrupación. Esta función se denomina grupos anidados. Actualmente, está permitido el anidamiento de grupos estáticos.

El anidamiento puede tener varios niveles, hasta 200.

Para obtener más información sobre los Grupos anidados, consulte la [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guía de administración de NetIQ eDirectory 8.8 SP8).

