IBM® SecureWay® Policy Director

Funcionamiento y ejecución

Versión 3 Release 0

SCT6-3KES-00

IBM® SecureWay® Policy Director

Funcionamiento y ejecución

Versión 3 Release 0

SCT6-3KES-00

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información general que aparece en el Apéndice A, “Avisos” en la página 77.

Primera edición (octubre de 1999)

Este manual es la traducción del original inglés Up and Running. Esta edición se refiere a la Versión 3, release 0, nivel de modificación 0 del producto IBM SecureWay Policy Director (SCT6-3KNA-00) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Esta edición sustituye a IBM SecureWay Global Sign-On, Versión 2.0.200.

Contenido

Acerca de este manual

Este manual proporciona información sobre la instalación y configuración de IBM® SecureWay® Policy Director (Policy Director). Los servidores de Policy Director pueden instalarse en los siguientes sistemas operativos:

- Microsoft® Windows NT®
- AIX®
- Solaris®

El cliente NetSEAT puede instalarse en los siguientes sistemas operativos:

- Windows® 95
- Windows 98
- Windows NT

Destinatarios de este manual

Este manual va dirigido al administrador que vaya a realizar la planificación e instalación de Policy Director.

El administrador debe tener conocimientos sobre la instalación y configuración de IBM Distributed Computing Environment (DCE) y Lightweight Directory Access Protocol (LDAP) de IBM SecureWay Directory. Policy Director utiliza los servidores de IBM SecureWay Directory e IBM Distributed Computing Environment que están incluidos en el producto Policy Director.

Organización de este manual

Este manual contiene los siguientes capítulos:

- El Capítulo 1, “Qué es Policy Director” en la página 1 ofrece una visión general de Policy Director y de sus componentes.
- El Capítulo 2, “Requisitos del sistema” en la página 11 proporciona información sobre los requisitos de software y hardware que debe cumplir el entorno operativo.
- El Capítulo 3, “Planificación para Policy Director” en la página 15 proporciona información para ayudarle a planificar, organizar y gestionar Policy Director.
- El Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23 proporciona información sobre la instalación y configuración de IBM SecureWay Directory Versión 3.1.1 (LDAP) Client SDK y servidor si elige el registro de usuarios LDAP. Debe instalar y configurar el servidor LDAP antes de instalar Policy Director. Además, el servidor LDAP debe estar en funcionamiento antes de instalar Policy Director.
- El Capítulo 5, “Instalación de Policy Director para Windows” en la página 35 describe la instalación y configuración de Policy Director en el sistema operativo Windows NT.
- El Capítulo 6, “Instalación de Policy Director para AIX” en la página 47 describe la instalación y configuración de Policy Director en el sistema operativo IBM AIX.

- El Capítulo 7, “Instalación de Policy Director para Solaris” en la página 61 describe la instalación y configuración de Policy Director en el sistema operativo Sun Solaris.
- El Capítulo 8, “Documentación relacionada” en la página 73 indica donde puede encontrar más información sobre Policy Director y documentación sobre productos relacionados.

Novedades de este release

Policy Director incluye las siguientes funciones nuevas en este release:

- Soporte para IBM SecureWay Directory para el almacenamiento de información de credenciales de usuarios y grupos.
- Las actualizaciones más recientes de Open Group para la especificación de la API de autorizaciones.
- Capacidad de definir y editar las credenciales de usuario proxy de IBM Firewall utilizando Policy Director Management Console.
- Un Policy Director Credentials Acquisition Service (CAS) que proporciona soporte para la utilización de servicios de autentificación externos.
- Soporte para la autentificación basada en certificados del área del cliente utilizando el nuevo Policy Director Credentials Acquisition Service.
- La capacidad de escribir su propio servicio de adquisición de credenciales personalizado utilizando la interfaz Interface Definition Language (IDL) entre WebSEAL y Policy Director CAS. Policy Director también proporciona la infraestructura general del servidor que gestiona las funciones del servidor de Policy Director CAS, como por ejemplo el arranque, el registro del servidor y el manejo de señales.
- La posibilidad de utilizar un mecanismo de tunelización de SSL (Secure Sockets Layer) además de la tunelización de GSS (Generic Security Services).
- Utilización de la interfaz de la línea de mandatos de Policy Director para gestionar las políticas de inicio de sesión y de contraseñas.
- Utilización de Policy Director Management Console, o la interfaz de la línea de mandatos, para gestionar usuarios, grupos y recursos (destinos) de conexión propia.
- Una herramienta de gestión de contraseñas de recursos de conexión propia basada en la Web.
- Un proceso de instalación integrado.

Preparación para el año 2.000

Estos productos están preparados para el año 2.000. Cuando se siguen las instrucciones indicadas en su documentación, pueden ejecutar, proporcionar y/o recibir datos de fechas correctos tanto del siglo veinte como del siglo veintiuno, siempre y cuando todos los elementos (por ejemplo hardware, software y firmware) utilizados con estos productos intercambien adecuadamente con ellos datos de fechas exactos.

Servicio y soporte

Póngase en contacto con IBM cuando necesite de servicio y soporte para cualquiera de los productos incluidos en la oferta IBM SecureWay FirstSecure. Algunos de estos productos pueden hacer referencia a soporte que no sea de IBM. Si ha

adquirido dichos productos como parte de la oferta FirstSecure, póngase en contacto con IBM para solicitar servicio o soporte.

Convenios

Este manual utiliza los siguientes convenios tipográficos:

Convenio	Significado
negrita	Elementos de la interfaz de usuario, como por ejemplo recuadros de selección, botones y elementos que hay dentro de cuadros de lista.
`monoespacio`	Sintaxis, código de ejemplo y cualquier texto que el usuario debe escribir.
Cursiva	Enfatización y primera utilización de términos especiales que sean importantes para Policy Director.
→	Muestra una serie de selecciones de un menú. Por ejemplo, pulse el botón en **Archivo → Ejecutar** significa pulse el botón en **Archivo** y después pulse el botón en **Ejecutar**.

Información en la Web

La información sobre actualizaciones de última hora de Policy Director se encuentra en la siguiente dirección de la Web:

`http://www.ibm.com/software/security/policy/library`

La información sobre actualizaciones de otros productos IBM SecureWay FirstSecure se encuentra en la siguiente dirección de la Web:

`http://www.ibm.com/software/security/firstsecure/library`

Capítulo 1. Qué es Policy Director

IBM SecureWay Policy Director (Policy Director) está disponible como un componente de IBM SecureWay FirstSecure o como un producto autónomo.

Qué es IBM SecureWay FirstSecure

IBM SecureWay FirstSecure (FirstSecure) forma parte de las soluciones de seguridad integradas de IBM. FirstSecure es un conjunto completo de productos integrados que permiten a su empresa realizar lo siguiente:

- Establecer un entorno de e-business seguro.
- Reducir el coste total de propiedad de la seguridad simplificando la planificación de la seguridad.
- Implementar una política de seguridad.
- Crear un entorno efectivo de e-business.

Los productos de IBM SecureWay incluyen:

Policy Director
IBM SecureWay Policy Director (Policy Director) proporciona autentificación, autorización, seguridad de los datos y gestión de los recursos de la Web.

Boundary Server
IBM SecureWay Boundary Server (Boundary Server) proporciona las siguientes funciones:

- Las funciones más importantes de cortafuegos tales como filtrado, proxy y pasarela a nivel de circuito
- Una conexión de VPN (Red privada virtual) con IBM Firewall
- Componentes para la seguridad en Internet
- Una solución de seguridad de código móvil

Una GUI de configuración une la función de usuario proxy de Policy Director con el producto Firewall de Boundary Server.

Intrusion Immunity
Intrusion Immunity proporciona detección de intrusiones y protección antivirus.

Trust Authority
IBM SecureWay Trust Authority (Trust Authority) cumple los estándares de la PKI (Public Key Infrastructure) para criptografía e interoperatividad. Trust Authority proporciona soporte para la emisión, renovación y revocación de certificados digitales. Estos certificados proporcionan un medio de autentificar a los usuarios y de asegurar unas comunicaciones fiables.

Toolbox
IBM SecureWay Toolbox (Toolbox) es un conjunto de interfaces de programación de aplicaciones (API) con las cuales los programadores de aplicaciones pueden incorporar seguridad en el software. Puede obtener Toolbox como parte de FirstSecure. Tanto Policy Director como Toolbox incluyen la biblioteca y documentación de API de Policy Director.

Dado que cada producto de IBM SecureWay FirstSecure puede instalarse independientemente, puede planificar una transición controlada hacia un entorno seguro. Esta posibilidad reduce la complejidad y el coste de proteger su entorno y acelera el despliegue de aplicaciones y recursos de la Web.

Consulte la documentación de FirstSecure *Planificación e integración* para obtener más información sobre los componentes de FirstSecure y para obtener una lista de la documentación del producto IBM SecureWay.

Qué es IBM SecureWay Policy Director

Policy Director es una solución autónoma de gestión de seguridad y autorizaciones que proporciona protección, de principio a fin, de los recursos para intranets y *extranets* geográficamente dispersas. Una *extranet* es una red privada virtual (Virtual Private Network, VPN) que utiliza funciones de control de acceso y de seguridad para restringir la utilización de una o más intranets conectadas a Internet para determinados abonados.

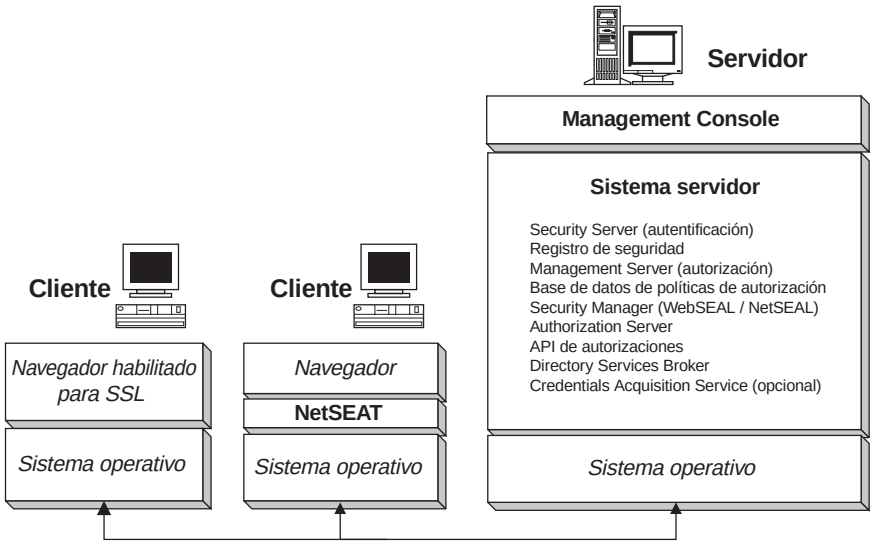
Policy Director proporciona autentificación, autorización, seguridad de los datos y servicios de gestión de recursos. Puede utilizar Policy Director junto con aplicaciones basadas en Internet para crear intranets y extranets seguras y bien gestionadas.

Policy Director se ejecuta en los sistemas operativos Windows NT, AIX y Solaris.

Componentes de Policy Director

Policy Director incluye los siguientes componentes:

- Clientes y servidores de Lightweight Directory Access Protocol (LDAP) de IBM SecureWay Directory e IBM Distributed Computing Environment (DCE)
- Policy Director Base
- Management Server
- Security Manager, formado por WebSEAL y NetSEAL
- Credential Acquisition Service (CAS)
- Authorization Server
- Interfaz de programación de aplicaciones (API) de autorizaciones
- Cliente NetSEAT
- Management Console
- Directory Services Broker (DSB)



Antes de instalar Policy Director, debe determinar qué posibilidades de seguridad y de gestión necesita su red. Utilice los apartados siguientes para decidir qué componentes de Policy Director necesita.

Servidores de IBM SecureWay Directory y DCE

Policy Director utiliza los servidores de IBM SecureWay Directory e IBM Distributed Computing Environment que están incluidos en el producto Policy Director.

Policy Director puede utilizar un registro de usuarios LDAP o un registro de usuarios DCE. Durante la instalación de Policy Director, el sistema le pedirá que seleccione el tipo de registro de usuarios.

Si tiene la intención de utilizar un registro de usuarios LDAP, debe instalar un cliente LDAP y configurar un servidor LDAP antes de instalar Policy Director. Siga las instrucciones del Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23. Si tiene la intención de utilizar un registro de usuarios DCE, puede saltarse el apartado que explica cómo instalar y configurar LDAP.

Servidor de IBM SecureWay Directory

SecureWay Directory proporciona el LDAP (Lightweight Directory Access Protocol) para mantener la información de directorios en una ubicación central para almacenamiento, actualizaciones, recuperación e intercambio. Si utiliza LDAP para su registro de usuarios, Policy Director utiliza LDAP para otorgar autorización a los usuarios.

Servidor de IBM Distributed Computing Environment

Distributed Computing Environment (DCE) incluye servicios y herramientas que permiten la creación, utilización y mantenimiento de aplicaciones distribuidas en un entorno informático heterogéneo. DCE forma el dominio seguro dentro del cual los servidores de Policy Director pueden autentificar mutuamente el usuario y comunicarse de forma segura. En el sistema operativo Windows NT, el cliente NetSEAT funciona igual que el cliente DCE.

Policy Director Base

El componente Policy Director Base (IVBase) es el software de referencia común que utilizan todos los componentes de Policy Director. Este componente se instala automáticamente cuando se instalan otros componentes de Policy Director, excepto cuando se instala Management Console en Windows.

Para AIX, el componente SMIT Setup (IV.Smit) se incluye como parte del paquete de IV.Base. Este paquete contiene información de configuración que utiliza el SMIT. Este paquete debe instalarse en todos los servidores de AIX.

Management Server

Management Server (IVMgr) es el servidor de autorizaciones principal de todo el dominio seguro. Management Server controla y mantiene la base de datos maestra de políticas de autorización. Todos los datos fluyen a través de Management Server.

Management Server debe instalarse en un sistema del dominio seguro antes de instalar Security Managers o Authorization Servers, pero no necesariamente en el mismo sistema. Debe haber una sola instancia de Management Server instalada en un dominio seguro determinado.

Cada instancia de Management Server requiere la instalación de los siguientes componentes en el mismo sistema que Management Server:

- Cliente DCE
- Cliente LDAP (si está utilizando LDAP como registro de usuarios)
- Policy Director Base
- Management Server

Security Manager

Security Manager (IVNet) aplica una política de control de accesos basada en la información procedente de una réplica de una base de datos de políticas de autorización. Security Manager incluye los siguientes componentes:

- WebSEAL para un control de accesos estricto de Hypertext Transfer Protocol (HTTP) y de la interfaz Secure Sockets Layer (HTTPS)
- NetSEAL para un control de accesos flexible de Transmission Control Protocol/Internet Protocol (TCP/IP)

Los componentes NetSEAL y WebSEAL son necesarios para configurar y habilitar estas posibilidades, que por omisión están inhabilitadas.

WebSEAL

WebSEAL (IVWeb) es el componente del servidor HTTP de Security Manager. WebSEAL es un servidor Web seguro que ofrece soporte para clientes HTTP, HTTPS y NetSEAT. WebSEAL se combina con Policy Director Credential Acquisition Service (CAS) para dar soporte a la autentificación basada en certificados X.509 para un usuario de Policy Director.

NetSEAL

NetSEAL (IVTrap) proporciona un control de accesos flexible para servidores TCP/IP. NetSEAL controla el acceso a un conjunto de puertas configuradas de un servidor TCP/IP.

La suite de productos de Policy Director proporciona seguridad para el intercambio de datos cliente/servidor a través de Internet y de intranets privadas. Policy Director NetSEAL y Policy Director WebSEAL son productos del área del servidor que controlan y gestionan datos de la red dentro de dominios seguros definidos por DCE.

Authorization Server

Authorization Server (IVAcld) atiende a las peticiones de autorización de las aplicaciones de terceros que utilizan la API de autorizaciones de Policy Director en modalidad remota. Authorization Server debe instalarse en al menos un sistema del dominio seguro para las aplicaciones de terceros.

Interfaz de programación de aplicaciones de autorizaciones

El componente Policy Director Authorization Application Development Kit o ADK (IVAuthADK) incluye las interfaces de programación de aplicaciones (API) de autorizaciones de Policy Director. La API permite crear aplicaciones que utilizan la autorización de Policy Director.

Policy Director Application Development Kit (ADK) incluye un servidor de la API de autorizaciones (AuthAPI™) que permite a los programadores incorporar directamente la seguridad y autorizaciones de Policy Director en las aplicaciones de la empresa. La API de autorizaciones de Policy Director permite el acceso directo a Policy Director Authorization Service. Utilizando esta API de autorizaciones, ya no es necesario que los programadores escriban código de autorización para cada aplicación.

El ADK incluye programas de ejemplo de C.

El ADK también contiene la fuente para el servidor de demostración de Policy Director Credential Acquisition Service (CAS) y para el servidor de demostración del servicio de autorizaciones externo.

Cliente NetSEAT

El cliente Policy Director NetSEAT es un cliente ligero para Windows 95, Windows 98 o Windows NT. NetSEAT proporciona canales de comunicación seguros a los servidores de Policy Director.

El software del cliente NetSEAT permite que los clientes se incorporen a dominios seguros y utilicen los servicios de seguridad avanzados que ofrecen los servidores WebSEAL y NetSEAL. NetSEAT protege todas las comunicaciones de red de un cliente, permitiendo el cifrado, de principio a fin, de todo el tráfico cliente/servidor y basado en Web.

NetSEAT ofrece la capacidad de proteger el tráfico TCP/IP de un cliente como el que generan servicios tales como Telnet y POP3. NetSEAT permite que un administrador del sistema ejerza un control flexible de las actividades de la red de una estación de trabajo. Este control se consigue gracias a la utilización de la

capacidad del dominio seguro de autentificar a usuarios y de asignar privilegios a usuarios y recursos.

Management Console

Management Console (IVConsole) es una aplicación gráfica basada en Java que se utiliza para gestionar la política de seguridad del dominio seguro de Policy Director. Con Management Console, se pueden realizar tareas administrativas en el registro de contabilidad y en la base de datos primaria de políticas de autorización. Management Console requieres que un cliente DCE inicie una sesión en el dominio seguro y que realice RPC seguras a Policy Director Management Server. Management Console utiliza servicios DCE ligeros (servicios de ejecución) que proporciona el cliente NetSEAT en Windows 95, Windows 98 o Windows NT.

Directory Services Broker

Directory Services Broker (DSB) se distribuye como parte del componente Management Server. Los clientes Management Console y NetSEAT requieren un DSB en el dominio seguro cuando se ejecutan en una estación de trabajo con Windows 95, Windows 98 o Windows NT. Normalmente, DSB no requiere operaciones de administración ni de configuración tras la instalación inicial.

Credentials Acquisition Service (opcional)

Policy Director Credentials Acquisition Service (CAS) es un componente que se configura opcionalmente.

La *adquisición de credenciales* es el proceso en el que la información específica de una identidad proporcionada por un mecanismo de autentificación se correlaciona o transforma en una representación común, para todo el dominio, de la identidad del cliente. Esta representación común se denomina *credenciales de cliente*.

Cuando sea necesaria la adquisición o correlación de credenciales, deberá configurarse Policy Director Credentials Acquisition Service para poder utilizarlo con Policy Director WebSEAL Server. WebSEAL correlaciona automáticamente los usuarios de Policy Director con credenciales.

Los clientes que accedan a Policy Director utilizando certificados X.509 del área del cliente podrán correlacionar la información de *certificados* con identidades de Policy Director a través de Policy Director Credentials Acquisition Service o escribiendo un servicio propio de adquisición de credenciales.

Si hay usuarios que están definidos en algún otro registro externo, los nombres de usuario pueden correlacionarse con identidades de Policy Director mediante la utilización de un servidor CAS personalizado. Puede escribir y personalizar su propio servidor CAS para proporcionar una solución específica para el dominio seguro y procesar información de autentificación como, por ejemplo, certificados de clientes, nombres de usuarios o señales. El programador o diseñador de Policy Credentials Acquisition Service determina completamente los datos específicos de este servicio de autentificación y correlación. Policy Director almacena las normas de correlación en una base de datos externa de Policy Director. Policy Director proporciona la interfaz Interface Definition Language (IDL) entre WebSEAL y Policy Director Credentials Acquisition Service. Policy Director también proporciona la infraestructura general del servidor que gestiona funciones del servidor de Policy Director Credentials Acquisition Service como, por ejemplo, el arranque, el registro del servidor y el manejo de señales. Es responsabilidad del

programador de Policy Director Credentials Acquisition Service ampliar la infraestructura del servicio de adquisición de credenciales para que lleve a cabo las funciones de correlación de identidades que necesite la aplicación.

Para obtener más información sobre cada uno de los componentes de Policy Director, consulte la publicación *Policy Director Guía de administración*.

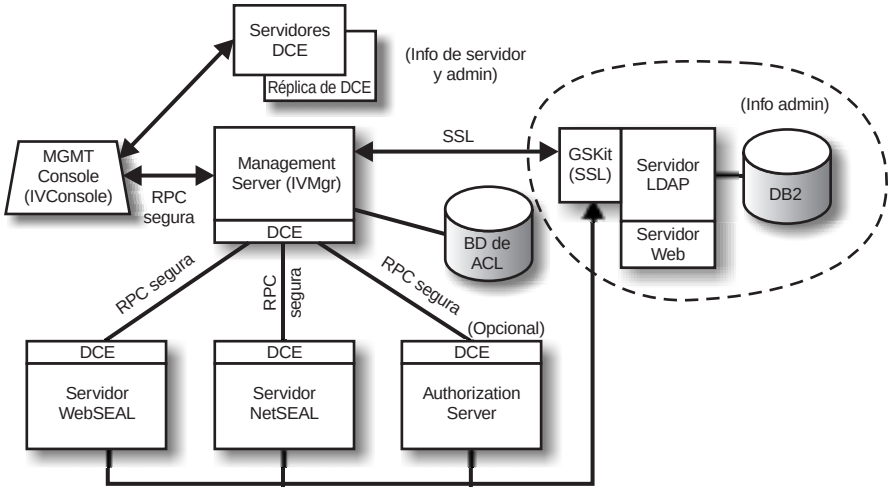
Cómo funciona Policy Director

Los apartados siguientes muestran cuatro ejemplos que describen los usos más habituales de Policy Director:

- Un administrador que utiliza Management Console
- Un usuario que accede a los recursos protegidos de la Web desde un navegador Web
- Un usuario que accede a un servidor TCP/IP protegido utilizando un cliente NetSEAT
- Un usuario que accede a un servidor de terceros protegido

Tareas de administración utilizando Management Console

La figura siguiente muestra cómo fluyen los datos cuando un administrador utiliza Management Console para gestionar Policy Director. Los componentes de LDAP, que aparecen dentro de la línea punteada, sólo son necesarios si LDAP se utiliza como registro de usuarios.



Un administrador de Management Console se autentifica en el dominio seguro y recibe credenciales.

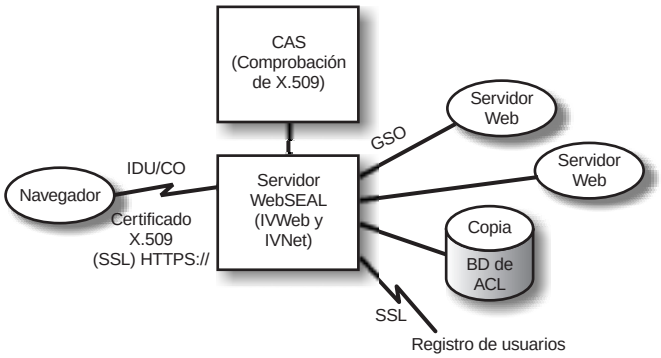
Cuando el administrador gestiona usuarios o grupos de Management Console, Management Console envía peticiones a través de una RPC segura a Management Server. Management Server envía los cambios correspondientes al servidor LDAP a través de una conexión SSL que se ha establecido previamente utilizando el nombre distinguido (DN) y la contraseña de Management Server.

Cuando el administrador añade, notifica o aplica una lista de control de acceso (ACL), Management Console envía los datos a través de una RPC segura a Management Server. A continuación, Management Server almacena los cambios en la copia local de la base de datos de ACL. Cuando se modifica la base de datos de

ACL necesaria, Management Server notifica a los demás servidores a través de una RPC segura que la base de datos de ACL ha cambiado. Los servidores WebSEAL, NetSEAL y Authorization Server también comprueban periódicamente con Management Server las actualizaciones en la base de datos de ACL.

Usuario que accede a los recursos protegidos de la Web desde un navegador Web

La figura siguiente muestra cómo fluyen los datos cuando un usuario accede a los recursos protegidos de la Web desde un navegador Web.



Cuando el usuario intenta acceder a una página protegida de la Web, el navegador habilitado para SSL se pone en contacto con el servidor WebSEAL. Si WebSEAL se ha configurado para efectuar autentificaciones basadas en certificados de clientes, WebSEAL solicita al navegador un certificado X.509. Cuando WebSEAL recibe el certificado del navegador, lo pasa al servidor CAS. CAS intenta correlacionar el certificado que ha recibido con una identidad de usuario que Policy Director pueda entender. Dentro del archivo de configuración de CAS, el administrador de Policy Director puede crear una tabla que se utilice para asociar un DN de certificado con el DN de un usuario de Policy Director. Cuando WebSEAL llama a CAS con un certificado, primero extrae el DN del certificado y comprueba si hay alguna coincidencia en la tabla. Si encuentra una coincidencia, el CAS devuelve a WebSEAL el DN de usuario asociado de Policy Director. WebSEAL utiliza entonces ese DN para identificar al usuario de Policy Director. Si no se encuentra ninguna coincidencia, el CAS devuelve el DN del certificado a WebSEAL. En ese caso, se utiliza el DN del certificado para identificar al usuario de Policy Director. WebSEAL Server usa el DN devuelto para recuperar las credenciales del usuario.

Para obtener más información sobre los certificados X.509, visite la siguiente dirección Web:

`http://www.ietf.org`

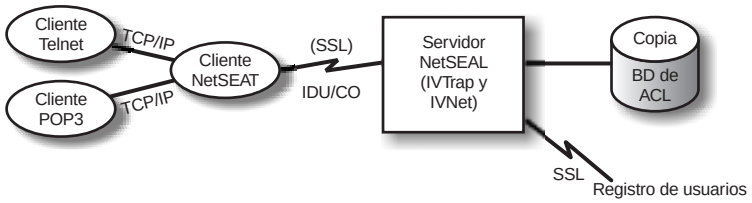
Cuando WebSEAL finaliza satisfactoriamente la autentificación del usuario, WebSEAL utiliza la réplica local de la base de datos de ACL para decidir si el usuario está autorizado para acceder al objeto Web de la forma solicitada.

Si la conexión entre el servidor WebSEAL y el servidor principal que contiene el recurso de la Web al que se accede es una conexión (junction) Global Sign-On (GSO), WebSEAL busca las credenciales GSO de dicha conexión (junction) en LDAP y pasa el nombre de usuario y contraseña al servidor Web.

Para obtener información sobre cómo gestionar recursos GSO y grupos de recursos GSO, consulte la información de Management Console en la publicación *Policy Director Guía de administración*.

Usuario que accede a un servidor TCP/IP protegido utilizando un cliente NetSEAT

La figura siguiente muestra cómo fluyen los datos cuando un usuario accede a un servidor TCP/IP protegido utilizando un cliente NetSEAT.



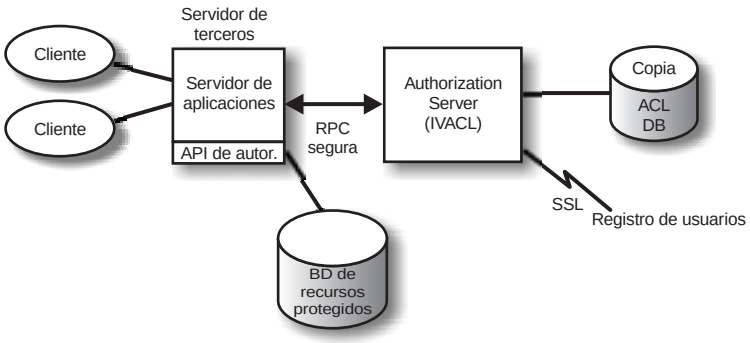
El usuario del cliente Telnet establece una comunicación TELNET con un servidor protegido por NetSEAL, el cual identifica que el usuario pide acceso. NetSEAL solicita el nombre de usuario y contraseña y verifica la identidad del usuario proporcionando la información del usuario y comparándola con el valor almacenado en el registro de usuarios. NetSEAL verifica que el usuario puede acceder al sistema a través de la puerta especificada.

NetSEAT redirige de forma transparente las peticiones a servidores de Policy Director enviando la información a través de un túnel SSL seguro. NetSEAT utiliza su información de configuración para reconocer las peticiones a un servidor seguro efectuadas desde aplicaciones TCP/IP genéricas, tales como Telnet, POP3 o HTTP. NetSEAT utiliza autentificación básica a través de SSL para establecer la identidad y credenciales del usuario de NetSEAT. Después de que se haya establecido la autorización, la SSL segura encapsula y completa la transacción solicitada de acuerdo con los valores de seguridad aplicables.

Por ejemplo, cuando un navegador Web solicita acceso a un servicio o recurso protegido por Policy Director Security Manager, NetSEAT intercepta de forma transparente la petición y la direcciona al servidor apropiado. Si ésta es la primera petición a Policy Director y necesita autentificación, NetSEAT visualiza para el usuario un recuadro de diálogo de inicio de sesión. Cuando un usuario se ha autentificado, Policy Director adjunta de forma transparente las credenciales apropiadas a cada petición de información que se realice en el futuro. Este proceso habilita un entorno de conexión propia para todas las aplicaciones Winsock que gestiona Policy Director. Además, Policy Director utiliza estas credenciales para determinar si el usuario puede acceder al recurso protegido de Policy Director que se ha solicitado.

Usuario que accede a un servidor de terceros protegido

La figura siguiente muestra cómo fluyen los datos cuando un usuario accede a un servidor de terceros protegido.



Cuando un cliente intenta acceder a datos protegidos de un servidor de terceros protegido, el servidor de terceros autentifica el usuario y correlaciona el usuario con un usuario de Policy Director. El servidor de aplicaciones pasa la información del usuario de Policy Director a Authorization Server, el cual se pone en contacto con LDAP (u otro producto, como por ejemplo DCE, que se utilice para el registro de usuarios) y recupera las credenciales del usuario. A continuación, el servidor de aplicaciones pasa las credenciales, el nombre del objeto que el usuario quiere acceder y la operación que el usuario quiere realizar a Authorization Server, el cual devuelve una indicación sobre si debe permitirse la operación. Entonces, el servidor de aplicaciones permite o deniega el acceso.

Qué contiene el paquete de Policy Director

El producto IBM SecureWay Policy Director, Versión 3.0, se suministra en cinco CD. Los títulos y el contenido de los CD se indican en la tabla siguiente.

Título del CD	Contenido
IBM SecureWay Policy Director Versión 3.0	• IBM Policy Director Versión 3.0
IBM SecureWay Policy Director Security Services	• IBM DCE para AIX Versión 2.2 • IBM DCE para Windows NT Versión 2.2 • Transarc DCE para Solaris Versión 2.0
IBM SecureWay Directory Versión 3.1.1 para AIX	• IBM SecureWay Directory Versión 3.1.1 • IBM DB2 Versión 5.2 con Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit Versión 3.0.1 (GSKit)
IBM SecureWay Directory Versión 3.1.1 para NT	• IBM SecureWay Directory Versión 3.1.1 • IBM DB2 Versión 5.2 con Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit Versión 3.0.1 (GSKit)
IBM SecureWay Directory Versión 3.1.1 para Solaris	• IBM SecureWay Directory Versión 3.1.1 • IBM DB2 Versión 5.2 con Fix Pack 8 • IBM Global Security Kit SSL Runtime Toolkit Versión 3.0.1 (GSKit)

Capítulo 2. Requisitos del sistema

El entorno operativo debe cumplir los requisitos de software y hardware que se describen en los apartados siguientes. Para obtener la información más reciente sobre los requisitos del sistema, consulte el archivo README de Policy Director. El archivo README contiene información que reemplaza a las publicaciones del producto.

Para obtener el archivo README más actual, acceda a la página de bibliotecas del sitio Web de IBM SecureWay Policy Director.

`http://www.ibm.com/software/security/policy/library`

Antes de instalar los componentes DCE, LDAP, NetSEAT y de servidor de Policy Director, asegúrese de que tiene el hardware y software necesario, que se detalla en los apartados siguientes.

Requisitos de hardware

La gestión de antememoria, almacenamiento intermedio y uso de memoria así como las estructuras de control son escalables. Sin embargo, los requisitos subyacentes del sistema operativo base, los requisitos de los clientes DCE y LDAP de requisito previo y los requisitos de las aplicaciones de cliente dictan los requisitos mínimos de espacio en disco y de memoria para la configuración.

Los requisitos de hardware del servidor de Policy Director son los siguientes:

Plataforma	Espacio en disco mínimo	Memoria mínima
Servidor Windows NT, con procesador Intel 80486 o compatible de 133 MHz o superior	16 MB	64 MB
Servidor AIX, hardware que ejecute AIX 4.3.1	16 MB	64 MB
Servidor Solaris, con hardware que ejecute Solaris 2.6	16 MB	64 MB

Los requisitos de hardware del cliente de Policy Director son los siguientes:

Plataforma	Espacio en disco mínimo	Memoria mínima
Cliente Windows NT, con procesador Intel 80486 o compatible de 133 MHz o superior	16 MB	32 MB
Servidor AIX, hardware que ejecute AIX 4.3.1	16 MB	32 MB
Servidor Solaris, con hardware que ejecute Solaris 2.6	16 MB	24 MB

Requisitos de software

Cuando planifique la instalación de Policy Director, asegúrese de que tiene las versiones correctas de los sistemas operativos y de otro software de requisito previo, que se muestran en los apartados siguientes. A continuación se indican los requisitos de sistema operativo para los servidores de Policy Director, el cliente NetSEAT y Management Console:

Servidores de Policy Director

Los servidores de Policy Director pueden instalarse en los siguientes sistemas operativos:

- Windows NT Server Versión 4.0 con Service Pack 4 o superior
- AIX Versión 4.3.1 o superior
- Sun Solaris Versión 2.6

Clientes NetSEAT

Los clientes de Policy Director NetSEAT pueden instalarse en los siguientes sistemas operativos:

- Windows NT Versión 4.0 con Service Pack 4 o superior
- Windows 98
- Windows 95

Management Console

Policy Director Management Console puede instalarse en los siguientes sistemas operativos:

- Windows NT Server, Versión 4.0, con Service Pack 4, o superior
- Windows NT, Windows 95 o Windows 98
- AIX Versión 4.3.1 o superior, que incluye Java Runtime 1.1.6 o superior
- Sun Solaris Versión 2.6

Otros requisitos de software

Policy Director requiere un servidor DCE y, si está utilizando LDAP como registro de usuarios, un servidor LDAP. Un servidor (LDAP o DCE) debe estar en al menos un sistema del dominio seguro. Los clientes DCE y LDAP se incluyen como parte del producto Policy Director. Puede instalarlos antes de instalar Policy Director, o bien puede utilizar una instalación existente de DCE y LDAP que esté en el nivel correcto.

Windows NT y AIX

En las plataformas Windows NT y AIX, los servidores de Policy Director requieren el siguiente software:

- IBM DCE para Windows NT Versión 2.2 o superior para servidores de Windows NT, o bien IBM DCE para AIX Versión 2.2 o superior para servidores de AIX
- IBM SecureWay Directory Versión 3.1.1 (LDAP), que incluye DB2® Versión 5.2, Fix Pack 7. LDAP sólo es necesario si se utiliza LDAP para el registro de usuarios.
- Secure Sockets Layer (SSL) Versión 3.0 o superior.
- Policy Director Credentials Acquisition Service (CAS) y WebSEAL requieren uno de los siguientes navegadores de la Web:
  - Microsoft Internet Explorer Versión 4 o superior
  - Netscape Communicator Versión 4.5 o superior
  - Netscape Navigator Versión 4.5 o superior
- Sólo para los clientes de Policy Director de Windows 95, se requiere Winsock Versión 2.0 o superior.

Solaris

En la plataforma Solaris, los servidores de Policy Director requieren el siguiente software:

- Transarc DCE Versión 2.0.
- IBM SecureWay Directory (LDAP) Versión 3.1.1, que incluye DB2 Versión 5.2, Fix Pack 8. LDAP sólo es necesario si se utiliza LDAP para el registro de usuarios.
- Secure Sockets Layer Versión 3.0 o superior.
- Policy Director CAS y WebSEAL requieren uno de los siguientes navegadores de la Web:
  - Microsoft Internet Explorer Versión 4 o superior
  - Netscape Communicator Versión 4.5 o superior
  - Netscape Navigator Versión 4.5 o superior

Capítulo 3. Planificación para Policy Director

En los apartados siguientes encontrará la información necesaria para preparar y planificar la instalación y configuración de Policy Director. Lea el Capítulo 1, “Qué es Policy Director” en la página 1 y decida qué componentes de Policy Director necesita antes de planificar la instalación.

Configuraciones comunes

Las configuraciones que aparecen en este apartado pueden ayudarle a determinar la configuración apropiada para su red. Utilice la tabla del apartado “Componentes necesarios para las configuraciones comunes” en la página 16 para determinar los componentes que necesita para su configuración. A continuación, seleccione estos componentes durante la instalación de Policy Director. Tenga en cuenta que WebSEAL y NetSEAL pueden instalarse en cualquier sistema. En la lista siguiente se indican algunas configuraciones comunes de componentes de Policy Director:

Sólo Management Server
: Un servidor que ejecuta la única instancia de Management Server para el dominio seguro. En este caso, Management Server reside solo en su propio sistema. Management Server mantiene la base de datos maestra de autorizaciones para el dominio seguro, replica esta base de datos en todo el dominio seguro y mantiene la información de ubicaciones sobre otros sistemas de servidores de Policy Director del dominio seguro.

Security Manager con el servidor WebSEAL
: WebSEAL está formado por dos componentes—Security Manager (IVNet) y WebSEAL (IVWeb). Un servidor WebSEAL protege un espacio de la Web. WebSEAL ofrece soporte a servidores principales para alta disponibilidad y tolerancia de errores mediante *smart junctions* o conexiones (junctions).

Security Manager con el servidor NetSEAL
: NetSEAL está formado por dos componentes—Security Manager (IVNet) y NetSEAL (IVTrap). Un servidor NetSEAL protege una VPN (Red privada virtual) y proporciona control de acceso para servicios de red heredados y de terceros.

Security Manager con el servidor WebSEAL y NetSEAL
: Un servidor WebSEAL y NetSEAL combinado.

Authorization Server
: Un servidor que proporciona acceso al servicio de autorizaciones de Policy Director para aplicaciones de terceros, utilizando la API de autorizaciones de Policy Director.

Authorization Server y ADK
: Un servidor que proporciona un entorno de desarrollo para desarrolladores que desean crear aplicaciones de terceros que utilicen la API de autorizaciones de Policy Director para llamar al servicio de autorizaciones.

Management Console
: Una aplicación gráfica basada en Java que se utiliza para gestionar la política de seguridad del dominio seguro de Policy Director. No se requiere IVBase para Management Console en Windows.

Todos los componentes
Un servidor que proporciona los servicios combinados de todas las configuraciones anteriores.

Componentes necesarios para las configuraciones comunes

Las configuraciones de Policy Director que se describen en el apartado “Configuraciones comunes” en la página 15 aparecen en la tabla siguiente. La tabla muestra los componentes que deben instalarse para cada configuración. Leyendo de izquierda a derecha, los componentes indicados están en el orden correcto de instalación.

Tenga en cuenta que dos componentes forman tanto WebSEAL como NetSEAL:

WebSEAL Security Manager (IVNet) y WebSEAL (IVWeb)

NetSEAL Security Manager (IVNet) y NetSEAL (IVTrap)

Notas para IVBase:

- No se requiere IVBase para Management Console en Windows.
- IV.Smit se instala automáticamente con IV.Base en AIX.

Ejemplos	Paquetes de instalación							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
Sólo la instancia única de Management Server	X	X						
Security Manager con WebSEAL	X	X***	X	X				
Security Manager con NetSEAL	X	X***	X		X			
Security Manager con WebSEAL y NetSEAL	X	X***	X	X	X			
Authorization Server	X	X***				X		
Authorization Server y ADK	X	X***				X	X	
Management Console	X							X
Todos los componentes	X	X***	X	X	X	X	X	X

*** Si es el primer o único sistema del dominio seguro, debe instalar Management Server (IVMgr). Si es un sistema adicional de un dominio seguro existente con un Management Server existente, no debe instalar otro Management Server. Sólo debe haber un Management Server en un dominio seguro determinado.

Información necesaria antes de instalar

Antes de empezar a instalar Policy Director, tome nota de la información del sistema que es necesaria para instalar el software de Policy Director:

Servidores de Policy Director

- Nombre de usuario del administrador de célula (cell_admin)
- Contraseña del administrador de célula (cell_admin)
- WebSEAL: puerta HTTP (valor por omisión)
- WebSEAL: directorio root del documento de la Web

Cliente NetSEAT (sólo Windows)

- Nombre de célula
- Nombre del sistema principal de Security Server
- Nombre del sistema principal de Time Server
- Nombre del sistema principal de Directory Services Broker

Mecanismos de tunelización ("tunnel")

Policy Director soporta los siguientes protocolos para la transmisión de datos cifrados:

- Tunelización de Secure Socket Layer (SSL)
- Tunelización de Generic Security Services (GSS)

WebSEAL tiene soporte para la integridad y la privacidad de datos que proporciona el túnel ("tunnel") cifrado por SSL. WebSEAL y NetSEAL tienen soporte para RPC. Con la RPC, la utilización de la integridad y las indicaciones de la hora proporcionan protección contra *"reproducciones para usurpación de identidad"*. Una reproducción para usurpación de identidad se produce cuando los datos de un usuario se capturan mientras fluyen entre el cliente de dicho usuario y el servidor. A continuación, los datos se reproducen o vuelven a presentarse al servidor como medio de usurpar la personalidad del primer usuario.

Tunelización ("tunnel") de SSL: El protocolo SSL permite el intercambio de señales para establecer comunicaciones entre dos estaciones de trabajo. Este protocolo proporciona seguridad y privacidad en Internet. SSL funciona utilizando una clave pública para la autentificación y una clave secreta para cifrar los datos que se transfieren por la conexión SSL.

Habilite SSL cuando utilice la tunelización ("tunnel") de SSL para servidores Policy Director NetSEAL. Esta configuración se utiliza cuando un cliente NetSEAT presta servicio a un cliente SSL para un servidor Policy Director NetSEAL que tiene puertas específicas de seguridad (por ejemplo, la puerta utilizada por Telnet).

Policy Director WebSEAL tiene soporte para las Versiones 2 y 3 de SSL.

Tunelización ("tunnel") de GSS: La interfaz Generic Security Service, (GSS API) es una forma estándar que permite a las aplicaciones acceder a los servicios de seguridad. La tunelización ("tunnel") de GSS se utiliza a través de RPC seguras. Habilite esta opción cuando instale el cliente NetSEAT como módulo de soporte para Policy Director para Microsoft® Windows NT® o Policy Director Management Console.

La tunelización de GSS proporciona servicios de forma genérica a quienes efectúan llamadas. Tiene soporte con varios mecanismos y tecnologías subyacentes. Permite la portabilidad a distintos entornos de aplicaciones a nivel fuente. La tunelización habilita control sobre el nivel de protección en el tráfico del recorrido en ambas direcciones independientemente. Por ejemplo, el recorrido de los datos desde el cliente al servidor puede estar completamente protegido por un cifrado general de los datos, mientras que el recorrido de los datos que van del servidor al cliente puede no estar protegido.

Requisitos de instalación para el dominio seguro

Policy Director es un sistema de seguridad muy distribuido cuyos componentes pueden instalarse en diversas configuraciones en uno o más sistemas. La lista siguiente muestra los componentes que deben instalarse en el dominio seguro.

- Servicios DCE
- Un registro de usuarios. (IBM SecureWay Directory sólo es necesario si se utiliza LDAP para el registro de usuarios)
- Servidores de Policy Director
- Policy Director Management Console
- Policy Director Authorization ADK

Si utiliza una instalación existente de DCE o LDAP, asegúrese de que la instalación existente está en el nivel correcto. Consulte el apartado “Otros requisitos de software” en la página 12 para saber cuáles son los niveles correctos. Tenga en cuenta las siguientes dependencias antes de instalar el producto Policy Director.

Servicios DCE (Distributed Computing Environment)

Cada dominio seguro de Policy Director (célula DCE) requiere una instalación completa de los servicios DCE en al menos un sistema para proteger las comunicaciones entre los servidores de Policy Director. Los servicios DCE pueden residir en el mismo sistema principal que los servidores de Policy Director o bien pueden estar ubicados en un sistema principal remoto de la red.

Para obtener información sobre la instalación de DCE, consulte los manuales de instalación y administración así como los recursos de asistencia técnica para las plataformas que necesite. Consulte el apartado “Documentación de IBM Distributed Computing Environment” en la página 74 para ver una lista de documentación sobre DCE.

Siga las directrices que se indican a continuación cuando instale DCE:

- Si está creando un nuevo dominio seguro de Policy Director en un único sistema principal, realice una instalación completa del servidor DCE
- Si los servidores DCE se encuentran en un sistema principal remoto, cree un nuevo dominio seguro instalando Policy Director en un sistema principal local.
- Si está instalando Policy Director para Windows NT en un dominio seguro existente de Policy Director, utilice el cliente NetSEAT para facilitar el acceso a los servicios DCE necesarios. Instale el cliente NetSEAT en el mismo sistema principal que los servidores de Policy Director para Windows NT.

Registro de usuarios

Policy Director puede utilizar el registro de usuarios IBM SecureWay Directory (LDAP) o bien el registro de usuarios DCE como su registro de usuarios.

Si utiliza LDAP como registro de usuarios, debe tener un servidor LDAP instalado y configurado antes de instalar Policy Director y también debe instalar un cliente LDAP en cada sistema de Policy Director.

Consulte la publicación *IBM SecureWay Directory Installation and Configuration, Version 3.1.1* para obtener información sobre la instalación de LDAP. Consulte el apartado "Documentación de IBM SecureWay Directory" en la página 75 para saber cuál es la ubicación de esta documentación de LDAP.

O bien, consulte la información del producto DCE, que aparece en el apartado "Documentación de IBM Distributed Computing Environment" en la página 74, para obtener información sobre la instalación de DCE.

Servidores de Policy Director

Los siguientes requisitos se refieren a la instalación de los servidores de Policy Director.

- Para comunicarse correctamente, todos los servidores de Policy Director para Windows NT requieren el cliente Policy Director NetSEAT.
- Todas las instalaciones de servidores de Policy Director requieren el componente base, que se instala automáticamente.
- Si instala el *primer* o *único* sistema del dominio seguro, debe instalar Management Server en el sistema.
- Si instala un sistema *adicional* en un dominio seguro existente que tiene un Management Server existente, no instale otro Management Server. Debe haber una sola instancia de Management Server en un dominio seguro determinado.
- Los componentes Authorization Server de terceros, WebSEAL y NetSEAL son opcionales.
- Security Manager se combina con WebSEAL para proporcionar el componente del servidor HTTP de WebSEAL y el control de accesos estricto de HTTP, y con NetSEAL para proporcionar el componente de control de accesos flexible de TCP/IP de NetSEAL.
- Todos los servidores de Policy Director en AIX y Solaris requieren un cliente DCE completo y, si está utilizando LDAP como registro de usuarios, un cliente LDAP.

Management Console

Management Console requiere que el dominio seguro y Management Server estén instalados y configurados. Management Console también requiere un cliente DCE y, si está en un sistema Windows, el cliente NetSEAT.

Authorization ADK

Instale el Policy Director Authorization ADK en el sistema de desarrollo de aplicaciones. El Authorization ADK puede utilizarse para desarrollar aplicaciones que permiten a los usuarios acceder a servidores protegidos de terceros. El Authorization ADK requiere el componente base, que se instala automáticamente cuando se instala el Authorization ADK.

El dominio seguro en el que se ejecuta la aplicación debe tener instalado un Authorization Server en al menos un sistema. Un entorno de desarrollo típico incluye el Authorization Server en el mismo sistema que el Authorization ADK.

Visión general de la instalación paso a paso de Policy Director

La instalación de Policy Director requiere realizar los siguientes pasos:

1. Si tiene instalada un versión anterior de IBM SecureWay Policy Director y desea migrar su instalación, consulte la información sobre migración en la página Web de Policy Director (vea el apartado “Información en la Web” en la página vii).
2. Verifique que su sistema operativo tiene soporte para Policy Director.

   Consulte el apartado “Servidores de Policy Director” en la página 12 para obtener información sobre sistemas operativos soportados.
3. Determine qué componentes de servidor satisfacen mejor sus requisitos y en qué sistemas va a instalar dichos componentes.

   Consulte el apartado “Configuraciones comunes” en la página 15 para obtener asistencia.
4. Decida si el dominio seguro utilizará tunelización de SSL o tunelización de GSS.

   Consulte el apartado “Mecanismos de tunelización ("tunnel")” en la página 17 para obtener más información.
5. Instale y configure una infraestructura DCE, si no existe ninguna.

   Consulte el apartado “Servicios DCE (Distributed Computing Environment)” en la página 18 para tener una visión general de los servicios DCE necesarios.
6. Decida si el dominio seguro utilizará un registro de usuarios LDAP o un registro de usuarios DCE. Si está utilizando el IBM SecureWay Directory (LDAP) para su registro de usuarios y no está utilizando un LDAP existente, instale y configure LDAP.

   Consulte el apartado Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23 para obtener instrucciones sobre la instalación de LDAP.
7. Instale los clientes DCE y LDAP en los sistemas que se utilizarán para los servidores de Policy Director.

   Consulte la información del producto DCE, que aparece en el apartado “Documentación de IBM Distributed Computing Environment” en la página 74, para obtener información sobre la instalación de DCE.
8. Instale los componentes de servidor de Policy Director.

   Consulte el capítulo sobre instalaciones para la plataforma de sistema operativo que vaya a utilizar. Consulte uno de los siguientes capítulos:
   - Capítulo 5, “Instalación de Policy Director para Windows” en la página 35
   - Capítulo 6, “Instalación de Policy Director para AIX” en la página 47
   - Capítulo 7, “Instalación de Policy Director para Solaris” en la página 61
9. Configure Policy Director Credentials Acquisition Service (CAS) si va a utilizar Policy Director CAS para la autentificación de certificados de clientes.

   En el apartado “Configuración de Credentials Acquisition Service” en la página 21 encontrará información sobre Policy Director CAS.

10. Instale Management Console.

    Consulte el capítulo sobre instalaciones para la plataforma de sistema operativo que vaya a utilizar. Consulte uno de los siguientes capítulos:

    - Para Windows NT, consulte el apartado “Instalación de Management Console en Windows” en la página 42.
    - Para AIX, consulte el apartado “Instalación de Management Console” en la página 57 si está utilizando el registro de usuarios DCE, o bien el apartado “Configuración y arranque de Management Console” en la página 51 si está utilizando el registro de usuarios LDAP.
    - Para Solaris, consulte el apartado “Instalación de Management Console” en la página 70.

Reinstalación de Policy Director

Si debe reinstalar algún paquete, primero debe eliminar el paquete existente y, a continuación, reinstalar el paquete deseado. Consulte el apartado “Eliminación de Policy Director” en la página 58 para ver las instrucciones.

Configuración de Credentials Acquisition Service

Policy Director Credentials Acquisition Service (CAS) es un componente personalizable de Policy Director que puede utilizarse para ampliar los mecanismos de autentificación estándar soportados por WebSEAL.

Policy Director CAS se instala automáticamente. Si desea utilizar Policy Director CAS como su servicio de adquisición de credenciales, debe configurarlo. Consulte el capítulo 2 y el capítulo 13 de la publicación *Policy Director Guía de administración* para obtener información sobre que es y cómo se configura Policy Director CAS.

Capítulo 4. Instalación y configuración de IBM SecureWay Directory

Si tiene la intención de utilizar un registro de usuarios DCE, puede saltarse este apartado sobre la instalación y configuración de IBM SecureWay Directory (LDAP).

Durante la instalación de Policy Director, se le pedirá que elija un registro de usuarios LDAP o un registro de usuarios DCE.

- Si elige LDAP, deberá instalar un IBM SecureWay Directory Versión 3.1.1 (LDAP) Client SDK y servidor, y después configurar el servidor LDAP antes de instalar Policy Director.
- Si utiliza SSL para acceder al servidor LDAP, también deberá configurar el cliente LDAP.

Instalación del servidor y cliente LDAP

Policy Director requiere un servidor y cliente LDAP si está utilizando LDAP como su registro de usuarios.

Un servidor LDAP debe estar en al menos un sistema del dominio seguro. El cliente y servidor LDAP se incluyen como parte del producto Policy Director. Debe instalarlos antes de instalar Policy Director, o bien puede utilizar una instalación existente de LDAP que esté en el nivel correcto.

Durante la instalación de LDAP, elija **SecureWay Directory and Client SDK**.

Para obtener más información sobre la instalación y configuración de LDAP, consulte la documentación de *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*. Existe una versión distinta de este manual, en formato HTML, para cada sistema operativo soportado en su CD correspondiente. Consulte el apartado “Documentación de IBM SecureWay Directory” en la página 75 para obtener información sobre cómo acceder a dicha documentación.

Instalación de sólo el cliente LDAP

Si utiliza LDAP como su registro de usuarios, debe instalar el cliente LDAP en cada sistema que ejecutará Policy Director. El cliente LDAP se incluye como parte del producto Policy Director. Instale el cliente LDAP antes de instalar Policy Director.

Durante la instalación de LDAP, elija **SecureWay Client SDK** sólo si ya tiene una instalación existente del servidor LDAP que esté en el nivel correcto ya instalado y configurado para Policy Director.

Configuración del servidor LDAP

Si utiliza LDAP como su registro de usuarios, debe configurar el servidor LDAP antes de instalar el primer servidor de Policy Director. Después de configurar el servidor LDAP para el primer sistema de Policy Director, no es necesario que vuelva configurar el servidor LDAP cuando añada servidores adicionales de Policy Director.

Si ha habilitado el acceso SSL al servidor LDAP durante la configuración del servidor LDAP, deberá copiar un par de anillo de claves cliente y servidor en cada sistema adicional que utilice el acceso SSL. Consulte el apartado “Habilitación del acceso SSL (opcional)” en la página 26 para obtener más información.

Para configurar el servidor LDAP, debe completar los pasos de configuración de la siguiente lista sólo una vez para cada dominio seguro:

1. Añada los sufijos necesarios. Consulte el apartado “Añadir sufijos” para ver las instrucciones.
2. Instale los objetos y atributos del esquema de seguridad. Consulte el apartado “Instalación de objetos y atributos del esquema de seguridad” en la página 25.
3. Habilite el control de acceso a LDAP. Consulte el apartado “Habilitación del control de accesos de LDAP” en la página 33 para ver las instrucciones.
4. Habilite el acceso SSL. Consulte el apartado “Habilitación del acceso SSL (opcional)” en la página 26 para ver las instrucciones.

Si ha habilitado el acceso SSL, lleve a cabo los pasos del apartado “Configuración del cliente LDAP para el acceso SSL” en la página 31 cada vez que añada un cliente LDAP (servidor de Policy Director) que utilice SSL para acceder al servidor LDAP.

Nota: Los administradores de LDAP pueden especificar los valores de cifrado de contraseñas en la base de datos de LDAP. LDAP permite que las contraseñas se almacenen como texto transparente, lo cual podría plantear un riesgo para la seguridad. Consulte la documentación de LDAP para ver las instrucciones sobre cómo establecer los atributos de las contraseñas de usuario en el nivel de cifrado adecuado.

Añadir sufijos

En IBM SecureWay Directory, cree un nuevo sufijo completando los siguientes pasos:

1. Utilizando un navegador Web, acceda a la herramienta Web Administration de IBM SecureWay Directory Server en la siguiente dirección de la Web

   `http://nombreservidor/ldap`

   Inicie una sesión a través de la interfaz de la Web como administrador de LDAP (por ejemplo, `cn=root`).
2. Pulse el botón en: **Sufijos → Añadir un sufijo**.
3. En el campo **DN de sufijo**, debe añadir el sufijo:

   `secAuthority=Default`

   El objeto para `secAuthority=Default` se crea durante la configuración de Management Server.
4. Pulse el botón **Añadir un nuevo sufijo**.
5. Para añadir otro sufijo, pulse el enlace **Añadir un sufijo** para regresar a la ventana anterior.
6. Si es necesario, añada un sufijo para los usuarios de Policy Director y los datos de Global Sign-On (GSO). Por ejemplo:

   `o=IBM,c=US`

   Puede poner el nombre que quiera a los sufijos de una forma apropiada para su instalación, donde `o=` es el nombre abreviado de su organización y `c=` es el país.

Este paso crea sufijos para los datos GSO y para los usuarios y grupos. Estos sufijos se crean con la herramienta Web Administration de LDAP.

7. Pulse el botón **Añadir un nuevo sufijo**.
8. Repita el procedimiento para cada nuevo sufijo que desee añadir y que sea necesario para su organización.
9. Pulse en el enlace **reiniciar el servidor** de la página Web actual de la herramienta LDAP Administration para reiniciar el servidor LDAP cuando haya terminado de añadir sufijos.

Instalación de objetos y atributos del esquema de seguridad

Policy Director utiliza un conjunto de objetos y atributos de LDAP para mantener las credenciales del usuario dentro del servidor LDAP.

Utilice IBM SecureWay Directory Management Tool (DMT) para determinar si están instalados los objetos y atributos de seguridad. Instálelos si todavía no están presentes. DMT se instala como parte del paquete de IBM SecureWay Directory.

Para determinar si están instalados los objetos y atributos de Policy Director, lleve a cabo los siguientes pasos:

1. Inicie Directory Management Tool en un cliente LDAP.

   Nota: Si recibe un mensaje que le indica que no hay ninguna entrada para el sufijo secAuthority=Default, puede proceder de forma segura. El objeto para el sufijo secAuthority=Default se crea durante la configuración de Management Server.

2. Pulse el botón en **Esquema → Clases de objetos → Ver clases de objetos**.
3. Verifique la presencia de todos los objetos y atributos siguientes de Policy Director:

   Clases de objetos
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser

4. Pulse el botón **Esquema → Atributos → Ver atributos**
5. Verifique la presencia de todos los objetos y atributos siguientes de Policy Director:

   Atributos
   secUUID
   secLoginType
   secAuthority
   secAcctValid
   secPwdValid
   secDN
   secPwdMgmtBind
   secAcctExpires
   secAcctInactivity
   secAcctLife
   secPwdAlpha
   secPwdSpaces
   secPwdFailures
   secPwdLastChanged

secPwdLastUsed

6. Realice una de las siguientes acciones según los resultados del paso 3 en la página 25 y del paso 5 en la página 25.
   - Si todos los objetos están presentes, no es necesario realizar ninguna otra acción. Vaya al apartado “Habilitación del acceso SSL (opcional)”.
   - Si *algunos* de los objetos, pero no todos, están presentes, vaya al paso 7.
   - Si *ninguno* de los objetos está presente, vaya al paso 8.
7. Si se encuentran algunos de los objetos y atributos, pero no todos, de Policy Director, elimine los objetos y atributos existentes de Policy Director.

   En DMT, pulse el botón en:

   Esquema → Clases de objetos → Eliminar clases de objetos y elimine las clases de objetos.

   A continuación, pulse el botón en **Esquema → Atributos → Eliminar atributos** y elimine los atributos.
8. Si no se encuentra ninguno de los objetos y atributos de Policy Director, inserte el CD *IBM SecureWay Policy Director Versión 3.0*.
9. En el indicador de mandatos, utilice **ldapmodify** para cargar el archivo de esquemas. Por ejemplo, escriba:

   UNIX:

   ```
   ldapmodify -h nombre sistema principal -p 389 -D cn=root -w contraseña -f /schema/secschema.def
   ```

   Windows:

   ```
   ldapmodify -h nombre sistema principal -p 389 -D cn=root -w
   contraseña -f
   x:\schema\secschema.def
   ```

   donde *x:* es la letra de la unidad de CD-ROM de Windows.
10. Si tiene la intención de utilizar Policy Director para gestionar usuarios de SecureWay Boundary Server, también debe añadir los objetos y atributos del archivo de esquemas de Policy Director:

    En el indicador de mandatos, utilice el mandato **ldapmodify** para cargar el archivo de esquemas. Por ejemplo, escriba:

    Windows:

    ```
    ldapmodify
    -h nombre sistema principal -p 389 -D cn=root -w contraseña -f x:\schema\puschema.def
    ```

    UNIX:

    ```
    ldapmodify -h nombre sistema principal -p 389 -D cn=root -w  contraseña -f /schema/puschema.def
    ```

    donde *x:* es la letra de la unidad de su CD-ROM

Habilitación del acceso SSL (opcional)

Si el acceso SSL a su servidor LDAP no es necesario, sáltese este apartado. Vaya al apartado “Habilitación del control de accesos de LDAP” en la página 33.

Si su servidor LDAP necesita el acceso SSL, siga leyendo este apartado. Este procedimiento sólo debe realizarse la primera vez que se establece la comunicación SSL entre el servidor LDAP y el cliente LDAP.

Opcionalmente, puede habilitar el uso de SSL para proteger las comunicaciones entre los servidores de Policy Director y el servidor LDAP.

IBM Global Security Kit (GSKit) SSL Runtime Toolkit Versión 3.0.1 se instala durante la instalación de LDAP. GSKit proporciona dos versiones de Key Management Tool—una versión es para Windows (**ikmguiw**) y la otra versión no es para Windows (**ikmgui**). Puede utilizar cualquiera de las dos versiones siempre que **ikmguiw** se llame en los siguientes procedimientos.

Las instrucciones completas sobre cómo utilizar esta herramienta pueden encontrarse en la documentación de LDAP. Consulte el apartado “Documentación de IBM SecureWay Directory” en la página 75.

O bien, puede seguir estos procedimientos abreviados para habilitar específicamente Policy Director para el acceso SSL.

Creación del archivo de base de datos de claves y del certificado

Para habilitar el soporte de SSL en el servidor LDAP, el servidor debe tener un certificado que lo identifique y que pueda utilizarlo como un *certificado personal*. Este certificado personal es el certificado que el servidor envía al cliente para permitir que el cliente autentifique al servidor. Los certificados y el par de claves pública y privada se almacenan en un archivo de base de datos de claves. Un cliente normalmente adquiere un *certificado firmado* de una autoridad de certificación (CA), como por ejemplo VeriSign.

Sin embargo, también puede utilizar un certificado *auto-firmado*. Si se utiliza un certificado auto-firmado, la máquina en la que se genera el certificado se convierte en la CA.

Utilice Key Management Tool (**ikmguiw**) de GSKit para crear el archivo de base de datos de claves y el certificado. Para crear el archivo de base de datos de claves y el certificado (auto-firmado o firmado):

1. Asegúrese de que IBM Global Security Kit (GSKit) SSL Runtime Toolkit Versión 3.0.1 y la Key Management Tool basada en Java están instalados tanto en el servidor LDAP como en los clientes LDAP que utilizarán SSL.

   Windows: `C:\Archivos de programa\IBM\GSK\bin\ikmguiw.exe`

   Solaris: `/opt/IBM/GSK/bin/ikmguiw`

   AIX: `/usr/lpp/ibm/gsk/bin/ikmguiw`

2. Inicie IBM Key Management Tool (**ikmguiw**).
3. Pulse el botón en **Archivo de base de datos de claves → Nuevo**.
4. Verifique que el **archivo de base de datos de claves CMS** es el tipo de base de datos de claves seleccionado.
5. Escriba la información en los campos **Nombre de archivo** y **Ubicación** donde desea que se ubique el archivo de base de datos de claves. Una extensión del archivo de base de datos de claves es *.kdb*.
6. Pulse el botón en **Aceptar**.
7. Escriba la contraseña del archivo de base de datos de claves y confírmela.

   Recuerde esta contraseña ya que es necesaria cuando se edita el archivo de base de datos de claves.

8. Acepte la hora de caducidad por omisión, o bien cámbiela según los requisitos de su organización.
9. Si desea que la contraseña se enmascare y se almacene en un archivo stash, pulse el botón en **Guardar la contraseña en un archivo stash**.

   Algunas aplicaciones pueden utilizar un archivo stash de modo que la aplicación no tenga que saber la contraseña para utilizar el archivo de base de datos de claves. El archivo stash tiene la misma ubicación y nombre que el archivo de base de datos de claves y tiene la extensión *.sth*.
10. Pulse el botón en **Aceptar**.

Esto completa la creación del archivo de base de datos de claves. Hay un conjunto de certificados del firmante por omisión. Estos certificados del firmante son las Autoridades de certificación por omisión que están reconocidas.

Creación de un certificado personal

Si tiene la intención de utilizar un certificado de una autoridad de certificación (como por ejemplo VeriSign), debe solicitar el certificado a la CA y después recibirlo una vez que se ha completado. Siga los pasos del apartado “Recepción del certificado”.

Recepción del certificado: Si utiliza un certificado de una autoridad de certificación (como por ejemplo VeriSign) en lugar de un certificado auto-firmado, lleve a cabo los siguientes pasos:

1. Utilice **ikmguiw** para solicitar un certificado a una CA y después recibir el nuevo certificado en el archivo de base de datos de claves.
2. Pulse el botón en el apartado **Peticiones de certificados personales** del archivo de base de datos de claves.
3. Pulse el botón en **Nuevo**.
4. Cumplimente toda la información necesaria para generar una solicitud que pueda enviarse a la autoridad de certificación.
5. Pulse el botón en **Aceptar**.
6. Una vez que la CA devuelve el certificado, puede instalarlo en el archivo de base de datos de claves pulsando el botón en el apartado **Certificados personales** y después pulsando el botón en **Recibir**.
7. Una vez que tenga el certificado del servidor LDAP en el archivo de base de datos de claves, puede configurar el servidor LDAP para habilitar SSL.

Si su certificado todavía no está reconocido, copie el certificado de la CA en la máquina cliente.

Si su certificado está generado por una CA que ya está reconocida (como por ejemplo VeriSign), no es necesario realizar ninguna otra acción. Vaya al apartado “Configuración del servidor LDAP para habilitar SSL” en la página 30.

Creación de un certificado auto-firmado: Si tiene la intención de utilizar un certificado de una autoridad de certificación (como por ejemplo VeriSign) en lugar de un certificado auto-firmado, lleve a cabo los siguientes pasos.“Recepción del certificado”.

Para crear un nuevo certificado auto-firmado y almacenarlo en el archivo de base de datos de claves:

1. Pulse el botón en **Crear → Nuevo certificado auto-firmado**.

2. Escriba un nombre en el campo **Etiqueta de la clave** que GSKit pueda utilizar para identificar este nuevo certificado en la base de datos de claves.

   Por ejemplo, la etiqueta puede ser el nombre de la máquina del servidor LDAP.
3. Acepte los valores por omisión del campo **Versión**, que es X509 V3, y del campo **Tamaño de la clave**.
4. Acepte el nombre de la máquina por omisión, o bien escriba un nombre distinguido distinto en el campo **Nombre común** para este certificado.
5. Escriba un nombre de empresa en el campo **Organización**.
6. Complete los campos opcionales o déjelos en blanco.
7. Acepte los valores por omisión para el campo **País** y 365 para el campo **Período de validez**, o bien cámbielos según las necesidades de su organización.
8. Pulse el botón en **Aceptar**.

   GSKit genera un nuevo par de claves pública y privada y crea el certificado.

   Si tiene más de un certificado personal en el archivo de base de datos de claves, GSKit le pide si desea que esta clave sea la clave por omisión en la base de datos. Puede aceptar una de ellas como el valor por omisión. El certificado por omisión se utiliza en la ejecución cuando no se proporciona una etiqueta para seleccionar el certificado que se va a utilizar.

Esto completa la creación del certificado personal del servidor LDAP. Éste debe aparecer en el apartado Certificados personales del archivo de base de datos de claves. Utilice la barra del medio de Key Management Tool para seleccionar los tipos de certificados que se guardan en el archivo de base de datos de claves.

A continuación, debe extraer el certificado del servidor LDAP server en un archivo de datos ASCII con codificación Base64.

Extracción del certificado auto-firmado

Si su certificado está auto-firmado, debe extraer el certificado del firmante del archivo de base de datos de claves. Siga con este procedimiento de extracción.

Esta extracción se utiliza para configurar la máquina cliente. Si ha creado un certificado auto-firmado en el apartado “Creación de un certificado auto-firmado” en la página 28, también aparece en el apartado `Certificados del firmante` del archivo de base de datos de claves ya que es un certificado auto-firmado. Cuando se encuentre en el apartado Certificados del firmante de la base de datos de claves, verifique que el nuevo certificado está allí.

Para extraer el certificado del firmante:

1. Utilice **ikmguiw** para extraer el certificado del servidor LDAP en un archivo de datos ASCII con codificación Base64. Este archivo se utilizará en el procedimiento descrito en el apartado “Configuración del cliente LDAP para el acceso SSL” en la página 31.
2. Resalte el certificado auto-firmado que acaba de añadir en el apartado “Creación de un certificado auto-firmado” en la página 28.
3. Pulse el botón en **Extraer certificado**.
4. Pulse el botón en **datos ASCII con codificación Base64** como tipo de datos.
5. Escriba un nombre de archivo para el certificado que se acaba de extraer. La extensión del archivo del certificado es *.arm*.
6. Escriba la ubicación donde desea guardar el certificado extraído.

7. Pulse el botón en **Aceptar**.
8. Copie el certificado extraído en la máquina cliente LDAP.
9. Puede configurar el servidor LDAP para habilitar SSL.

Configuración del servidor LDAP para habilitar SSL

Para configurar el servidor LDAP para habilitar SSL:

1. Asegúrese de que el servidor LDAP está instalado y ejecutándose si va a utilizar LDAP como registro de usuarios. Consulte el Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23 para ver las instrucciones completas
2. Utilice la herramienta de administración de LDAP basada en la Web con el siguiente URL:

   `http://`*`nombreservidor`*`/ldap`

   Donde *nombreservidor* es el nombre de la máquina servidor LDAP.
3. Conéctese como administrador de LDAP (por ejemplo, cn=root) si todavía no estaba conectado.
4. Pulse el botón en **Servidor → SSL**.
5. Pulse el botón en **SSL activado**, que es para la habilitación SSL y no SSL, o bien pulse el botón **Sólo SSL** para el estado SSL que desee establecer.
6. Pulse el botón en **Autentificación de servidor** para el tipo de método de autentificación.
7. Escriba un número de puerta, o bien acepte el número de puerta por omisión de 636.
8. Escriba la vía de acceso de la base de datos de claves y el nombre de archivo que ha especificado en el paso 5 del apartado Creación del archivo de base de datos de claves y del certificado.

   La extensión del archivo de base de datos de claves es *.kdb*
9. Escriba el nombre en el campo **Etiqueta de la clave** que ha utilizado para identificarlo cuando ha almacenado el certificado del servidor LDAP en la base de datos de claves. Por ejemplo, la etiqueta podría ser el nombre de la máquina del servidor LDAP.
10. Escriba la contraseña del archivo de base de datos de claves y confírmela. O bien, puede dejar en blanco el campo de la contraseña si desea que el servidor LDAP utilice el archivo stash.
11. Pulse el botón en **Aplicar**.
12. Pulse el enlace **reiniciar el servidor** para reiniciar el servidor LDAP y hacer que este cambio surta efecto.

Prueba del acceso SSL: Para probar que SSL se ha habilitado, escriba el siguiente mandato desde la línea de mandatos del servidor LDAP:

```
ldapsearch -h nombreservidor -Z -K archivoclaves -P co_clave -b "" -s base \
objectclass=*
```

La barra inclinada invertida (\) de este mandato sólo es necesaria cuando el mandato no puede especificarse en una línea.

Donde:

Opción	Descripción
nombreservidor	El nombre del sistema principal DNS del servidor LDAP.
archivoclaves	El nombre completo de vía de acceso del anillo de claves generado.
co_clave	La contraseña del anillo de claves generado.

Este mandato devuelve la información base de LDAP, que incluye los sufijos del servidor LDAP.

La configuración SSL del servidor ha finalizado. A continuación, configure el cliente LDAP para el acceso SSL.

Configuración del cliente LDAP para el acceso SSL

Después de configurar el servidor LDAP para el acceso SSL, debe configurar los clientes LDAP para el acceso SSL.

Creación de un archivo de base de datos de claves: Asegúrese de que GSKit está instalado en el cliente y, a continuación, cree un nuevo archivo de base de datos de claves utilizando IBM Key Management Tool como se describe en el apartado "Creación del archivo de base de datos de claves y del certificado" en la página 27.

Para que el cliente pueda autentificar el servidor LDAP, el cliente debe reconocer a la autoridad de certificación (firmante) que ha creado el certificado del servidor LDAP. Si el servidor LDAP utiliza un certificado auto-firmado, hay que habilitar al cliente para que reconozca la máquina que ha generado el certificado del servidor LDAP como root fiable (autoridad de certificación).

Añadir un certificado del firmante: Para añadir un certificado del firmante una vez que se ha creado el archivo de base de datos de claves:

1. Asegúrese de que el certificado que se ha extraído del archivo de base de datos de claves del apartado "Extracción del certificado auto-firmado" en la página 29 se ha copiado en la máquina cliente. Si no se ha copiado, cópielo ahora.
2. Pulse el botón en el apartado **Certificados del firmante** del archivo de la base de datos de claves CMS del cliente.
3. Pulse el botón en **Añadir**.
4. Pulse el botón en **datos ASCII con codificación Base64** para establecer el tipo de datos.
5. Indique el nombre de archivo del certificado y su ubicación. La extensión del archivo del certificado es *.arm*.
6. Pulse el botón en **Aceptar**.
7. Escriba una etiqueta para el certificado del firmante que está añadiendo. Por ejemplo, es posible que desee utilizar el nombre de la máquina del servidor LDAP para la etiqueta.
8. Pulse el botón en **Aceptar**.

   El certificado auto-firmado aparece en la base de datos de claves del cliente como un certificado del firmante.

9. Resalte el certificado del firmante que acaba de añadir y pulse en botón en **Ver/Editar**.
10. Asegúrese de que está marcado como root fiable cerciorándose de que se ha seleccionado **Establecer el certificado como root fiable**.

    Si el certificado del servidor LDAP ha sido generado por una autoridad de certificación normal, asegúrese de que la autoridad de certificación esté listada como certificado del firmante y marcada como root fiable. En caso contrario, añada el certificado de la autoridad de certificación como certificado del firmante y después indique que es un root fiable.

En este punto, el cliente debería poder establecer una sesión SSL con el servidor LDAP.

Prueba de la habilitación SSL: Para probar que SSL se ha habilitado, escriba el siguiente mandato desde una línea de mandatos del cliente LDAP:

```
ldapsearch -h nombreservidor -Z -K archivoclaves_cliente -P co_clave -b "" \
-s base objectclass=*
```

La barra inclinada invertida (\) de este mandato sólo es necesaria cuando el mandato no puede especificarse en una línea.

Donde:

Opción	Descripción
nombreservidor	El nombre del sistema principal DNS del servidor LDAP.
archivoclaves_cliente	El nombre completo de vía de acceso del anillo de claves generado.
co_clave	La contraseña del anillo de claves generado.

Este mandato devuelve la información base de LDAP, que incluye los sufijos del servidor LDAP.

La configuración SSL ha finalizado.

Utilización del tipo de autentificación de cliente y servidor LDAP (opcional)

Este apartado sobre configuración es opcional:

1. Complete el procedimiento descrito en el apartado “Configuración del servidor LDAP para habilitar SSL” en la página 30. Sin embargo, en lugar de configurar el servidor LDAP para **Autentificación de servidor**, seleccione realizar **Autentificación de cliente y servidor**.

   En este caso, una vez que el servidor haya enviado su certificado al cliente y haya sido autentificado por el cliente, el servidor solicita el certificado del cliente. Si el servidor LDAP se configura para ambos, entonces es necesario establecer también un certificado para la máquina cliente.
2. En la máquina cliente, el establecimiento de un certificado para la máquina cliente se realiza tal como se describe en los siguientes procedimientos:
   - “Creación del archivo de base de datos de claves y del certificado” en la página 27
   - “Creación de un certificado auto-firmado” en la página 28 si su certificado es un certificado auto-firmado o “Recepción del certificado” en la página 28 si el certificado es un certificado del firmante.
   - “Extracción del certificado auto-firmado” en la página 29

- "Configuración del servidor LDAP para habilitar SSL" en la página 30

3. En el servidor LDAP, una vez que se ha creado el certificado personal del cliente y se ha añadido al archivo de base de datos de claves del cliente, la autoridad de certificación que ha creado dicho certificado del cliente debe ser reconocida como un certificado del firmante (root fiable). El certificado de la autoridad de certificación se añade a la base de datos de claves del servidor LDAP tal como se describe en el apartado "Añadir un certificado del firmante" en la página 31.

Prueba del acceso SSL: Una vez que el servidor LDAP reconoce la autoridad de certificación que ha creado el certificado personal del cliente, la configuración puede probarse utilizando el siguiente mandato:

```
ldapsearch -h nombreservidor -Z -K archivoclaves_cliente -P co_clave -N etiqueta_cliente \
-b "" \ -s base objectclass=*
```

La barra inclinada invertida (\) de este mandato sólo es necesaria cuando el mandato no puede especificarse en una línea.

Donde:

Opción	Descripción
nombreservidor	El nombre del sistema principal DNS del servidor LDAP.
archivoclaves_cliente	El nombre completo de vía de acceso del anillo de claves de cliente generado.
co_clave	La contraseña del anillo de claves generado.
etiqueta_cliente	La etiqueta asociada con la clave, si existe. Este campo es opcional y sólo es necesario si el servidor LDAP está configurado para realizar la autentificación de cliente y de servidor.

Este mandato devuelve la información base de LDAP, que incluye los sufijos del servidor LDAP. Observe que el parámetro **-N** indica la etiqueta que se ha especificado cuando el certificado personal del cliente se ha añadido al archivo de base de datos de claves del cliente.

No especifique la etiqueta de certificado del firmante del servidor LDAP. El parámetro **-N** indica a GSKit el certificado del cliente que se envía al servidor cuando es solicitado. Si no se especifica ninguna etiqueta, se envía el certificado personal por omisión cuando el servidor solicita el certificado del cliente.

La configuración SSL ha finalizado.

Habilitación del control de accesos de LDAP

Para completar la integración de la seguridad de Policy Director con el registro de usuarios LDAP, actualice las ACL de LDAP que controlan el registro de usuarios siguiendo los pasos que se indican continuación:

1. Inicie Directory Management Tool desde el cliente LDAP o desde el servidor LDAP pulsando el botón en **Inicio → Programas → IBM SecureWay Directory → Directory Management Tool**.
2. Vuelva a ejecutar el servidor:
   a. Pulse el botón en **Servidor → Volver a ejecutar**.
   b. Pulse en botón en **Autentificado**.
   c. Escriba el DN de usuario (por ejemplo, cn=root).

d. Escriba su contraseña.

e. Pulse el botón en **Aceptar**.

3. Pulse el botón en **Aceptar** o bien cierre las ventanas de los mensajes de aviso que aparezcan.
4. Otorgue al grupo de daemons de seguridad de Policy Director el control total sobre los sufijos creados en el apartado “Añadir sufijos” en la página 24.

   a. Pulse el botón en **Entradas → Añadir entrada**.

   b. Escriba el sufijo para la base de datos de usuarios de GSO y usuarios de Policy Director en el **RDN de entrada**. Por ejemplo:

      ```
      o=IBM,c=US
      ```

   c. Pulse el botón en **Organización**.

   d. Pulse el botón en **Siguiente**.

      Aparece la ventana Crear una entrada de LDAP.

   e. Añada la información correspondiente a su organización y, a continuación, pulse el botón **Crear**.

   f. Pulse el botón en **Árbol → Renovar árbol** y la nueva entrada debería aparecer ahora en Examinar árbol de directorios.
5. Otorgue el control total al grupo de daemons de seguridad de Policy Director añadiendo lo siguiente a la lista de propietarios de cada ACL de LDAP de control:

   ```
   cn=SecurityGroup,secAuthority=Default
   ```

   pulsando en el pestaña **ACL**.

   Aparecerá la ventana **Editar una ACL de LDAP**.

   a. Escriba `cn=SecurityGroup,secAuthority=Default` en el campo DN y luego pulse en **grupo** de la lista desplegable.

   b. Pulse el botón **Añadir**.

   c. Seleccione todos los recuadros de selección en Derechos otorgados para añadir, eliminar y clase.

   d. Cuando haya finalizado, pulse en **Cambiar** y `cn=SecurityGroup,secAuthority=Default` ahora debería aparecer en la lista de ACL para su DN de sufijo.

   e. Repita el procedimiento para cada sufijo si tiene que añadir más de uno en la lista de propietarios.

Ahora ha finalizado la configuración de LDAP.

Capítulo 5. Instalación de Policy Director para Windows

Los apartados de este capítulo explican cómo instalar y configurar Policy Director en las plataformas Windows y Windows NT soportadas.

Antes de empezar la instalación de Policy Director, revise la información del apartado “Antes de instalar Policy Director para Windows”.

Antes de instalar Policy Director para Windows

Antes de empezar la instalación de NetSEAT y Policy Director, lea la siguiente información:

- Antes de instalar NetSEAT y Policy Director, debe instalar y configurar inicialmente el servidor de Windows NT.
- Debe conocer las contraseñas para el administrador del dominio de Windows NT y para el administrador del dominio seguro (por ejemplo, la cuenta cell_admin). Asegúrese de obtener los privilegios de administrador.
- Si está creando una nueva célula DCE cuando instale los servidores de Policy Director en el sistema operativo Windows NT:
  - — También debe instalar y configurar un servidor DCE.
  - — Si utiliza LDAP para su registro de usuarios, también debe instalar y configurar un servidor LDAP.
- Familiarícese con toda la información referente al despliegue de Policy Director, tal como se describe en “Requisitos de instalación para el dominio seguro” en la página 18.

Instalación de NetSEAT y Policy Director

Antes de empezar la instalación de Policy Director, asegúrese de cerrar todas las aplicaciones. Una vez haya terminado de instalar Policy Director, debe cerrar y reiniciar el sistema.

Cumplimentación del inventario del dominio seguro

Durante la instalación, debe facilitar la siguiente información que es específica a la configuración de su dominio seguro:

- El nombre de su dominio seguro (célula DCE), por ejemplo cell_admin.
- Los nombres de los sistemas que proporcionan los siguientes servicios:
  - — Security
  - — Time
  - — Cell Directory Services (CDS)
  - — Directory Services Broker (DSB)

Instalación de NetSEAT

El archivo de instalación de Policy Director NetSEAT copia los archivos de NetSEAT en el disco duro e inicia automáticamente el programa de utilidad de configuración de NetSEAT.

Para instalar NetSEAT:

1. Conéctese como usuario con privilegios de administrador.
2. Inserte el CD *IBM SecureWay Policy Director Versión 3.0* en la unidad de CD-ROM.
3. Cambie al directorio \win32\client del CD.
4. Efectúe una doble pulsación en el archivo Setup.exe y se iniciará el programa InstallShield.
5. Cuando aparezca la ventana Elegir idioma de instalación, seleccione el idioma apropiado.
6. Pulse el botón en **Siguiente** y aparecerá la ventana Bienvenido a Policy Director.
7. Pulse el botón en **Siguiente**.
8. Cuando aparezca la ventana Elegir componentes a instalar, pulse el botón en **Cliente para productos del servidor de Policy Director**.
9. Pulse el botón en **Siguiente**.
10. Cuando aparezca la ventana Elegir el tipo de instalación, pulse el botón en **Habitual**.

    La ubicación por omisión para una instalación habitual es:

    ```
    c:\Archivos de programa\ibm\netseat\
    ```

    O bien si pulsa en **Personalizada** especifique la unidad y el directorio donde desea instalar NetSEAT.

    Aparece la ventana Elegir ubicación de destino.
11. Pulse el botón en **Siguiente**.

    Los archivos de NetSEAT se copian en la ubicación de NetSEAT por omisión de su disco duro. Aparece la ventana Configuración de NetSEAT.

Configuración de NetSEAT

Las tareas de configuración de NetSEAT proporcionan a NetSEAT información sobre el dominio seguro, como por ejemplo nombres, ubicaciones y servicios del servidor DCE.

Una vez que todos los archivos de NetSEAT se han copiado en el disco duro, aparece la ventana Configuración de NetSEAT (pestaña **Dominios seguros**).

Para configurar NetSEAT:

1. Para añadir una entrada a un dominio seguro nuevo, pulse el botón en **Añadir**.

   Aparece la ventana Dominio seguro nuevo.
2. Escriba el nombre del dominio seguro (célula DCE) al que pertenecerá NetSEAT, como por ejemplo cell_admin.
3. Seleccione el recuadro de selección **Habilitar GSS** o **Habilitar SSL**.
4. Pulse el botón en **Aceptar**.

   Aparecerá la ventana Propiedades del dominio seguro.
5. Para añadir un servidor DCE y los servicios que éste ofrecerá, pulse el botón en **Añadir**.

   Aparecerá la ventana Añadir un servidor DCE.

Utilice esta ventana para informar a NetSEAT de los servidores DCE existentes en el dominio seguro y de los servicios que proporcionan cada uno de ellos. Es posible que deba añadir más de un servidor DCE. Todos los servicios pueden estar en un sistema o estar divididos en varios sistemas.

Los casos posibles son los siguientes:

- **Dominio seguro nuevo (un sistema principal)**

  Si está creando un dominio seguro nuevo formado solamente por un sistema principal, dicho sistema principal proporciona todos los servicios DCE. Escriba el nombre del sistema principal en el campo **Nombre de la máquina**. Seleccione uno o más servicios. Seleccione DSB aunque todavía no se haya instalado.

- **Dominio seguro nuevo (más de un sistema principal)**

  Si está creando un dominio seguro nuevo y los servicios DCE están ubicados en otro sistema principal, el sistema principal local sólo proporcionará el servicio DSB. En este caso, primero añada el servidor DCE que proporciona los servicios DCE (Security, Time, CDS). A continuación, añada otro servidor DCE que se llame `sistema principal local` que represente al sistema local y seleccione el recuadro de selección DSB. Puede seleccionar DSB aunque todavía no se haya instalado.

- **Dominio seguro existente**

  Si está añadiendo Policy Director en un dominio seguro existente, añada el nombre del servidor DCE que proporciona Security, Time y CDS. A continuación, añada el nombre del servidor DCE que incluye el Policy Director Management Server que tiene instalado automáticamente el DSB. Seleccione el recuadro de selección DSB para dicho sistema. En este caso, todos los servicios, inclusive DSB, pueden estar ubicados en el mismo sistema principal.

6. Para cada servidor, escriba completamente el nombre de máquina DN de un servidor existente en el dominio seguro (por ejemplo, SFF98732.austin.ibm.com).
7. Para cada servidor, seleccione uno o más servicios para el servidor:
   - Security
   - DSB
   - Time
   - CDS
8. Pulse el botón en **Aceptar**.

   La ventana Propiedades del dominio seguro muestra la nueva entrada.
9. Si es necesario, repita el paso 5 en la página 36 hasta el paso 8 para añadir más servidores y servicios.
10. En la ventana Propiedades del dominio seguro, acepte la configuración por omisión del inicio de sesión avanzado de **Sólo inicio de sesión DCE**.

    El área de inicio de sesión integrado de la ventana Propiedades del dominio seguro no se utiliza en esta instalación de NetSEAT.
11. Pulse el botón en **Aceptar**.

    Aparece la ventana Configuración de NetSEAT.
12. Pulse el botón en **Aceptar**.

Aparece la ventana Es necesario reiniciar el sistema.

13. Pulse el botón en **Sí** para reiniciar el sistema.
14. Pulse el botón en **Aceptar**.

    Cuando ser reinicia el sistema, NetSEAT se inicia automáticamente. Aparece un icono de NetSEAT en la barra de tareas de Windows.

    La instalación y configuración de NetSEAT ha finalizado.

Verificación de la configuración del cliente NetSEAT

Antes de instalar el servidor de Policy Director, verifique que el cliente NetSEAT se ha configurado correctamente en el dominio seguro especificado. Utilice **netseat_ping** para determinar si los siguientes servicios están disponibles:

- Security Service
- Time Service
- Cell Directory Service
- Directory Services Broker (DSB)

Para verificar que el cliente NetSEAT puede comunicarse con los servicios necesarios, lleve a cabo los siguientes pasos:

1. Pulse el botón en **Inicio → Programas → NetSEAT → Inicio de sesión con NetSEAT** para iniciar la sesión como cell_admin.

   O bien, puede utilizar el mandato **netseat_login** de la línea de mandatos para iniciar la sesión.
2. No seleccione Inicio de sesión PKI a menos que sea específicamente necesario para su configuración.
3. Escriba el nombre de usuario y contraseña del administrador de Policy Director.
4. Pulse el botón en **Aceptar**.
5. En la línea de mandatos, utilice el mandato **netseat_ping** para obtener el estado de la configuración.

   Por ejemplo, si un cliente NetSEAT se configura en un dominio seguro que se llama "redback," obtenga el estado escribiendo el siguiente mandato en el indicador del DOS:

   ```
   netseat_ping -C redback
   ```

   Aparecerá una información parecida a la siguiente salida:

   ```
   /.../redback:
          SecurityServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          CdsServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          TimeServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          DsbServers:
                       ncacn_ip_tcp:redback[ ] not available
                       ncacn_ip_udp:redback[ ] not available
   ```

   Sin embargo, tenga en cuenta que DSB todavía no se estará ejecutando si tiene la intención de crear un dominio seguro nuevo. En este caso, la salida de

netseat_ping para DSB indicará `not available`. Esta indicación es la salida esperada para este caso. Puede proceder de forma segura con la instalación de Policy Director ya que la instalación del componente Management Server de Policy Director instalará, configurará e iniciará automáticamente el DSB. Si DSB ya se está ejecutando, la salida para DSB indicará `is available (v3.1)`.

6. Si otros servicios aparte de DSB no están disponibles, resuelva el problema antes de instalar los servidores de Policy Director.

Instalación de servidores de Policy Director

Antes de empezar a instalar los servidores de Policy Director, debe saber el nombre de usuario y la contraseña de un administrador.

Para instalar los componentes de servidor de Policy Director:

1. Asegúrese de que el servidor LDAP está instalado y ejecutándose si va a utilizar LDAP como registro de usuarios. Consulte el Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23 para ver las instrucciones completas
2. Inserte el CD *IBM SecureWay Policy Director Versión 3.0* en la unidad de CD-ROM.
3. Cambie al directorio `\win32\server` del CD.
4. Pulse en el archivo Setup.exe y se iniciará el programa InstallShield.
5. Cuando aparezca la ventana Elegir idioma de instalación, seleccione el idioma apropiado.
6. Pulse el botón en **Siguiente** y aparecerá la ventana Bienvenido a Policy Director.
7. Pulse el botón en **Siguiente**.

   Aparece la ventana Elegir ubicación de destino.
8. Acepte la ubicación del directorio por omisión para los archivos de programa o bien pulse el botón **Examinar** para crear o seleccionar otro directorio.

   La ubicación por omisión es: `C:\Archivos de programa\IBM\`

   Si ha instalado NetSEAT en una ubicación que no es la que aparece por omisión, instale los servidores de Policy Director en la misma ubicación.
9. Pulse el botón en **Siguiente**.

   Aparece la ventana Seleccionar componentes.
10. Seleccione los componentes apropiados de los servidores de Policy Director. Para obtener ayuda al realizar esta selección, consulte el apartado “Configuraciones comunes” en la página 15.

    Sólo debe haber una instancia de Policy Director Management Server (IVMgr) en el dominio seguro.
11. Pulse el botón en **Siguiente**.
12. Si no ha seleccionado WebSEAL, vaya al paso 14 en la página 40.

    Si ha seleccionado el componente WebSEAL (IVWeb), aparece la ventana Elegir ubicación root del documento de la Web. Esta ventana le pide la ubicación del directorio root de su espacio de la Web. Todos los recursos que pertenecen a su sitio Web residen en este directorio.
13. Acepte la ubicación del directorio root por omisión o bien pulse el botón **Examinar** para crear o seleccionar otro directorio. La ubicación por omisión es:

```
C:\...\IBM\Policy Director\www\docs
```

Los archivos de Policy Director ahora se copian del CD a su disco duro. Aparece la ventana Inicio de sesión del administrador del dominio seguro. Este paso es necesario para establecer las credenciales de seguridad y finalizar el proceso de configuración.

14. Complete el nombre y la contraseña del Administrador de célula DCE.
15. Si ha seleccionado el componente Management Server (IVMgr), el sistema le pide que seleccione **Registro LDAP** o **Registro DCE**.

    Si no ha seleccionado Management Server, el tipo de registro de usuarios se detecta automáticamente para el dominio seguro existente.

    - Si se detecta un registro de usuarios LDAP, la instalación continúa tal como se describe en el apartado "Utilización de un registro de usuarios LDAP".
    - Si se detecta un registro de usuarios DCE, la instalación continúa tal como se describe en el apartado "Utilización de un registro de usuarios DCE" en la página 41.
16. Pulse en una de las siguientes opciones para su registro de usuarios:
    - Si ha seleccionado **Registro de usuarios LDAP**, vaya al apartado "Utilización de un registro de usuarios LDAP".
    - Si ha seleccionado **Registro de usuarios DCE**, vaya al apartado "Utilización de un registro de usuarios DCE" en la página 41.

Utilización de un registro de usuarios LDAP

Si el dominio seguro de Policy Director utiliza un registro de usuarios LDAP, o si está instalando IVMgr y ha seleccionado **Registro LDAP**, aparece la ventana Información sobre el servidor LDAP.

1. Escriba la información necesaria para la configuración del servidor LDAP:
    - Nombre del sistema principal LDAP
    - Número de puerta
    - Número de puerta SSL (sólo necesario si se utiliza SSL para acceder al servidor LDAP)
    - DN de LDAP para la base de datos GSO (por ejemplo, o=ibm,c=us)
2. Pulse el botón en **Siguiente**.

    Aparece la ventana Comunicación con el servidor LDAP.
3. Elija habilitar o inhabilitar la comunicación SSL entre Policy Director y el servidor LDAP. Pulse el botón en **Sí** para habilitar la comunicación SSL o pulse el botón en **No** para inhabilitar la comunicación SSL.

    En el caso de Windows NT, la comunicación SSL se habilita una vez entre todos los servidores de Policy Director del sistema principal y el servidor LDAP.

    Si ha habilitado la comunicación SSL, vaya al paso 4.

    Si ha inhabilitado la comunicación SSL, vaya al paso 5 en la página 41.
4. Especifique valores para los siguientes indicadores:
    - Ubicación del archivo de claves SSL
    - DN del archivo SSL (etiqueta de la clave)
    - Contraseña del archivo de claves SSL

Consulte el apartado “Creación del archivo de base de datos de claves y del certificado” en la página 27 para obtener información.

5. Pulse el botón en **Siguiente**.

   Aparece la ventana Inicio de sesión del administrador de LDAP.

6. Complete la información sobre el nombre (por ejemplo, cn=root) y la contraseña del administrador de LDAP y luego pulse el botón en **Aceptar**.

   Los servidores se configuran y se arrancan. Este proceso puede durar varios minutos. Aparece la ventana Información del sistema que muestra el estado de los servidores, así como información de registro.

7. Pulse el botón en **Siguiente**.

   Aparece la ventana La configuración de Policy Director ha finalizado.

8. Pulse el botón en **Sí** para reiniciar.

   Si ha marcado **No** en la opción de reinicio, debe reiniciar Windows NT más tarde para completar el proceso de configuración. De este modo finaliza la instalación de Policy Director.

9. Pulse el botón en **Terminar**.

   El sistema le pide que reinicie el sistema.

Utilización de un registro de usuarios DCE

Si el dominio seguro de Policy Director utiliza un registro de usuarios DCE, o si está instalando IVMgr y ha seleccionado **Registro de usuarios DCE**, la instalación continúa como se describe a continuación.

1. Si ha seleccionado el componente WebSEAL (IVWeb), aparece la ventana Elegir ubicación root del documento de la Web. Esta ventana le pide la ubicación del directorio root de su espacio de la Web. Todos los recursos que pertenecen a su sitio Web residen en este directorio.

   Si no ha seleccionado WebSEAL, vaya al paso 3.

2. Acepte la ubicación del directorio root por omisión o bien pulse el botón **Examinar** para crear o seleccionar otro directorio. La ubicación por omisión es:

   ```
   C:\Archivos de programa\IBM\Policy Director\www\docs
   ```

3. Pulse el botón en **Siguiente**.

   Los archivos de Policy Director ahora se copian del CD a su disco duro. Aparece la ventana Inicio de sesión del administrador del dominio seguro.

4. Complete la información sobre el nombre y la contraseña del administrador de LDAP y luego pulse el botón en **Aceptar**.

   Los servidores se configuran y se arrancan. Este proceso puede durar varios minutos. Aparece la ventana Información del sistema que muestra el estado de los servidores, así como información de registro.

5. Pulse el botón en **Siguiente**.

   Aparece la ventana La configuración de Policy Director ha finalizado.

6. Pulse el botón en **Terminar**.

   El sistema le pide que reinicie el sistema.

7. Pulse el botón en **Sí** para reiniciar.

Si ha marcado **No** en la opción de reinicio, debe reiniciar Windows NT más tarde para completar el proceso de configuración. De este modo finaliza la instalación de Policy Director.

Configuración de Credentials Acquisition Service

Policy Director CAS se instala automáticamente. Si desea utilizar CAS para su servicio de adquisición de credenciales, debe configurarlo. Consulte la información sobre cómo configurar un servicio de adquisición de credenciales en la publicación *Policy Director Guía de administración* para obtener instrucciones.

Utilización de la detección de NetSEAL en Windows NT

Policy Director NetSEAL (IVTrap) detecta las peticiones realizadas en puertas específicas. Para utilizar la detección de NetSEAL, debe parar y reiniciar todas las aplicaciones que utilizan las puertas especificadas.

Para obtener más información sobre cómo configurar Policy Director NetSEAL para detectar puertas específicas, consulte la información general de NetSEAL en la publicación *Policy Director Guía de administración*.

Instalación de Management Console en Windows

Policy Director proporciona una Management Console que gestiona muchos componentes del sistema de seguridad de Policy Director desde un escritorio de cliente de Windows. Management Console puede instalarse en cualquiera de los siguientes sistemas operativos:

- Windows 95
- Windows 98
- Windows NT Versión 4.0, con Service Pack 4 o superior

Cada sistema operativo de Windows que ejecute Policy Director requiere el cliente Policy Director NetSEAT.

El cliente NetSEAT puede configurarse como un cliente de ejecución DCE o como un cliente para un servidor de Policy Director. Aunque cualquiera de las dos configuraciones anteriores es aceptable para Management Console, los servidores de Policy Director requieren todo el cliente para el servidor de Policy Director.

Si necesita reinstalar algún componente, debe eliminar el componente existente antes de reinstalarlo.

Instalación de Management Console con componentes de servidor

Una vez que se han instalado y configurado los componentes de servidor de Policy Director según se explica en el apartado “Instalación de servidores de Policy Director” en la página 39, lleve a cabo los siguientes pasos:

1. Inserte el CD *IBM SecureWay Policy Director Versión 3.0* en la unidad de CD-ROM.
2. Cambie al directorio \win32\Console.
3. Efectúe una doble pulsación en el archivo Setup.exe y se iniciará el programa InstallShield.

4. Cuando aparezca la ventana Elegir idioma de instalación, seleccione el idioma apropiado.
5. Pulse el botón en **Siguiente** y aparecerá la ventana Bienvenido a Policy Director.
6. Pulse el botón en **Siguiente** y aparecerá la ventana Elegir ubicación de destino.
7. Indique una ubicación donde desea instalar los archivos.

   Los archivos se copian en sus ubicaciones correctas del sistema Windows. Aparece una ventana informativa que indica que la instalación se ha realizado satisfactoriamente.
8. Si el sistema le pide si desea reiniciar Windows, pulse el botón en **sí**.
9. Pulse el botón en **Aceptar**.
10. Vaya al apartado "Cómo iniciar Management Console" en la página 44.

Instalación de Management Console sin componentes de servidor

Para habilitar la administración de la seguridad de Policy Director a partir de sistemas Windows adicionales, puede instalar Management Console en sistemas Windows que no tienen instalados los componentes de servidor de Policy Director. Cuando instale Management Console de este modo, el cliente NetSEAT puede configurarse como un cliente de ejecución DCE o como un cliente para un servidor de Policy Director.

Para instalar Management Console sin los componentes de servidor, vaya al sistema de escritorio de Windows y lleve a cabo los siguientes pasos:

1. Verifique que el sistema operativo de Windows es una plataforma con soporte. Consulte el apartado "Servidores de Policy Director" en la página 12.
2. Instale el cliente Policy Director NetSEAT. Siga las instrucciones del "Instalación de NetSEAT" en la página 35.
3. Verifique que el cliente NetSEAT está configurado correctamente en el dominio seguro en que se ejecutará Management Console. Consulte el apartado "Verificación de la configuración del cliente NetSEAT" en la página 38.
4. Inserte el CD *IBM SecureWay Policy Director Versión 3.0* en la unidad de CD-ROM.
5. Cambie al directorio \win32\Console
6. Efectúe una doble pulsación en el archivo Setup.exe y se iniciará el programa InstallShield.
7. Cuando aparezca la ventana Elegir idioma de instalación, seleccione el idioma apropiado.
8. Pulse el botón en **Siguiente** y aparecerá la ventana Bienvenido a Policy Director.
9. Pulse el botón en **Siguiente** y aparecerá la ventana Elegir ubicación de destino.
10. Indique una ubicación donde desea instalar los archivos.

    Los archivos se copian en sus ubicaciones correctas del sistema Windows. Aparece una ventana informativa que indica que la instalación se ha realizado satisfactoriamente.
11. Pulse el botón en **Aceptar** para completar la instalación
12. Para iniciar Management Console, vaya al apartado "Cómo iniciar Management Console" en la página 44.

Cómo iniciar Management Console

Para iniciar Management Console:

1. Asegúrese de que los servidores de Policy Director están instalados y ejecutándose.
2. Pulse el botón en **Inicio → Programas → Policy Director → Management Console.**

   Aparece la ventana Policy Director Management Console.
3. Inicie la sesión con Management Console como usuario con privilegios de administrador, como por ejemplo cell_admin.

Eliminación de Policy Director

Para eliminar los componentes de Policy Director, conéctese como administrador. Inicie la sesión con el dominio de Windows como usuario con credenciales de administrador. Por ejemplo:

```
dce_login cell_admin contraseña
```

Si intenta eliminar un componente sin las credenciales correctas del dominio seguro, aparecerá una ventana con el mensaje Error de autentificación.

Debe eliminar los componentes de Policy Director exactamente en el orden inverso al de la instalación. Utilice el icono **Agregar o quitar programas** del Panel de control para eliminar Policy Director.

Para desinstalar toda la instalación de Policy Director, realice los siguientes procedimientos en el orden indicado:

1. Elimine Management Console.
2. Elimine los componentes de servidor.
3. Elimine el cliente NetSEAT.

Eliminación de Management Console

Para eliminar Management Console:

1. Si Management Console se está ejecutando, ciérrela.
2. Vaya a **Agregar o quitar programas** en el Panel de control y pulse el botón en **Policy Director Management Console.**
3. Pulse el botón **Agregar o quitar**.
4. Cuando se le solicite, pulse el botón en **sí** para confirmar que desea eliminar el programa.
5. Pulse el botón en **Aceptar**.

Eliminación de los componentes de servidor

Para eliminar los componentes de servidor de Policy Director, debe obtener privilegios y credenciales y, después, eliminar los componentes.

Para eliminar componentes de servidor:

1. Asegúrese de que los servidores de Policy Director están instalados y ejecutándose.

2. Vaya a **Agregar o quitar programas** en el Panel de control y seleccione el primer componente de servidor de Policy Director que desea eliminar.
3. Elimine los componentes de servidor de Policy Director exactamente en el orden inverso que se han instalado.

   Por ejemplo, si instala todos los componentes, elimínelos en el siguiente orden:
   - Authorization ADK (IVAuthADK)
   - Authorization Server (IVAcld).
   - NetSEAL (IVTrap).
   - WebSEAL (IVWeb).
   - Security Manager (IVNet).
   - Management Server (IVMgr).
   - Base (IVBase). Este componente siempre se instala automáticamente.

   Policy Director Management Console puede eliminarse en cualquier momento. Para más información sobre el orden en que se instalan los componentes, consulte el apartado “Visión general de la instalación paso a paso de Policy Director” en la página 20.
4. Pulse el botón **Agregar o quitar**
5. Especifique el nombre de usuario y contraseña del administrador de LDAP cuando se le solicite.
6. Repita el paso 2 hasta el paso 5 para cada componente de servidor de Policy Director.
7. Pulse el botón en **Aceptar** cuando haya terminado.

Eliminación del cliente NetSEAT

Debe tener privilegios de administrador de Windows NT para eliminar componentes de Policy Director NetSEAT.

1. Vaya a **Agregar o quitar programas** en el Panel de control y después pulse en la pestaña **Instalar/desinstalar**.
2. En la ventana de lista de la pestaña, pulse el botón en **Cliente Policy Director NetSEAT**.
3. Pulse el botón en **Agregar o quitar**
4. Pulse el botón en **Aceptar**.

Capítulo 6. Instalación de Policy Director para AIX

Los apartados de este capítulo explican cómo instalar y configurar Policy Director en el sistema operativo AIX.

Antes de empezar la instalación de Policy Director, revise la información del apartado “Antes de instalar Policy Director para AIX”.

Antes de instalar Policy Director para AIX

Antes de empezar la instalación de NetSEAT y Policy Director, lea la siguiente información:

- Si está creando una nueva célula DCE cuando instale los servidores de Policy Director:
  - — También debe instalar y configurar un servidor DCE.
  - — Si utiliza LDAP para su registro de usuarios, también debe instalar y configurar un servidor LDAP.
- Familiarícese con toda la información referente al despliegue de Policy Director, tal como se describe en “Requisitos de instalación para el dominio seguro” en la página 18.

Instalación de Management Console

Policy Director proporciona una Management Console que puede utilizarse para gestionar todos los componentes del sistema Policy Director. Los administradores pueden instalar Management Console en un sistema AIX, en un sistema Windows o en ambos.

Management Console para AIX se distribuye en un paquete denominado IV.Console. Utilice la SMIT para instalar y configurar el paquete.

Instalación de Policy Director

Para instalar Policy Director en AIX, siga las instrucciones que se indican a continuación:

1. Asegúrese de que el servidor LDAP está instalado y ejecutándose si va a utilizar LDAP como registro de usuarios. Consulte el Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23 para ver las instrucciones completas
2. Inicie la sesión como root.
3. Inserte el CD *IBM SecureWay Policy Director Versión 3.0* en la unidad de CD-ROM.
4. Inicie la SMIT.
5. Pulse el botón en **Instalación y mantenimiento de software**.

   Aparece el menú Instalación y mantenimiento de software.
6. Pulse el botón en **Instalar y actualizar software**.

   Aparece el menú Instalar y actualizar software.

7. Pulse el botón en **Instalar y actualizar software por nombre de paquete**.

   Aparece la ventana Instalar y actualizar software por nombre de paquete.
8. Escriba el nombre del dispositivo desde el que está instalando el software.

   Por ejemplo:
   - Si está instalando desde un dispositivo de CD, podría escribir: `/dev/cd0`
   - Si está instalando desde un directorio de un servidor montado, podría escribir: `/mnt/user/lpp/IV`

     Una vez que ha escrito el nombre del dispositivo, aparece una ventana Lista con múltiples selecciones.
9. Pulse el botón en **IV**.

   Una ventana Lista con múltiples selecciones muestra la lista de paquetes de software de Policy Director.
10. Seleccione los paquetes que desea instalar.
    - Para instalar todos los paquetes de Policy Director, pulse la entrada **IV**.
    - Cuando sólo instale algunos de los paquetes de Policy Director, tenga en cuenta las dependencias de la instalación que se describen en el apartado “Requisitos de instalación para el dominio seguro” en la página 18.
11. Pulse el botón en **Aceptar**.

    Aparece la ventana Instalar y actualizar software por nombre de paquete del menú SMIT.
12. Pulse el botón en **sí** en el campo que está etiquetado:

    `¿Instalar AUTOMÁTICAMENTE el software de requisito?`

    Este paso asegura que los paquetes de Policy Director Base (IV.Base) y SMIT Setup (IV.smit) están instalados. Estos paquetes son software de requisito previo para los demás paquetes de Policy Director. Si elige establecer este campo en **no**, regrese al menú de selección de paquetes. Asegúrese de que ha seleccionado IV.Base y IV.Smit.
13. Establezca los otros campos en los valores apropiados para su instalación.
14. Pulse el botón en **Aceptar**.

    SMIT muestra mensajes de estado, como por ejemplo:
    - Verificación de la preinstalación de los paquetes de software de Policy Director.
    - El nombre de cada paquete durante la extracción de los archivos del paquete.
    - Creación de menús de configuración para cada paquete.
    - Un mensaje de estado que indica si la extracción de archivos ha finalizado satisfactoriamente.
15. Cuando haya finalizado la extracción de archivos, configure los paquetes de Policy Director utilizando la información del apartado “Configuración de Policy Director con un registro de usuarios LDAP” en la página 49. O bien, consulte el apartado “Configuración de Policy Director con un registro de usuarios DCE” en la página 54 si está utilizando el registro DCE.

Configuración de Policy Director con un registro de usuarios LDAP

Debe instalar los paquetes de software de Policy Director antes de configurarlos. Si todavía no ha instalado los paquetes de Policy Director, consulte el apartado “Instalación de Policy Director” en la página 47.

Si ha instalado Policy Director con un registro de usuarios DCE, vaya al apartado “Configuración de Policy Director con un registro de usuarios DCE” en la página 54.

Debe configurar cada paquete instalado de Policy Director, con la excepción de SMIT Setup. Configure los paquetes de uno en uno. Algunos de los paquetes de Policy Director requieren que el administrador responda a solicitudes de la pantalla durante la configuración.

Para configurar los paquetes de Policy Director:

1. Inicie la SMIT.

   Aparece el menú Gestión del sistema.
2. Pulse el botón en **Aplicaciones y servicios de comunicaciones**.

   Aparece una lista de paquetes de software instalados. Por ejemplo:
   - TCP/IP
   - NFS
   - DCE (Distributed Computing Environment)
   - Policy Director
3. Pulse el botón en **Policy Director**.

   Aparece el menú Policy Director con las siguientes opciones:
   - Configuración de Policy Director
   - Desconfiguración de Policy Director
4. Pulse el botón en **Configuración de Policy Director**.

   Aparece una lista de paquetes de Policy Director instalados, como por ejemplo:
   - Configuración de Policy Director Base
   - Configuración de Policy Director Management Server
   - Configuración de Policy Director Management Console
   - Configuración de Policy Director Security Manager
   - Configuración de Policy Director WebSEAL
   - Configuración de Policy Director Authorization Server
   - Configuración de Policy Director NetSEAL
   - Configuración de Policy Director Authorization ADK
5. Pulse en cada paquete que quiera configurar, de uno en uno.

   Debe configurar los paquetes de Policy Director en el orden en que aparecen en la lista de configuración de Policy Director. Seleccione cada paquete de uno en uno, desde el elemento superior al elemento inferior.

Ahora debe configurar los paquetes de Policy Director que ha seleccionado siguiendo las instrucciones de configuración pertinentes que se indican en los apartados siguientes.

Configuración del paquete Base

El paquete Base se instala en un sistema siempre que se instala cualquiera de los demás paquetes. Para configurar el paquete Base, pulse el botón en **Policy Director Base** en la lista de configuración de Policy Director.

La configuración del paquete Policy Director finaliza sin ninguna entrada de usuario.

Configuración de Management Server

Para configurar Management Server:

1. Pulse el botón en **Policy Director Management Server** en la lista de configuración de Policy Director.

   Aparece un indicador que le solicita que elija un tipo de registro de usuarios.
2. Si utiliza LDAP como su registro de usuarios, escriba `2` para el registro de usuarios LDAP.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
3. Cuando se le indique, escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   Si utiliza LDAP como su registro de usuarios, aparece una serie de indicadores para configurar la comunicación entre Management Server y el servidor LDAP.
4. Escriba la información necesaria para la configuración del servidor LDAP:
   - Nombre del sistema principal del servidor LDAP
   - Número de puerta del servidor LDAP
   - Número de puerta SSL del servidor LDAP (opcional)
5. Escriba el nombre de usuario y la contraseña del usuario administrativo de LDAP (por ejemplo, `cn=root`). La información de seguridad de Policy Director ahora se registra con el servidor LDAP.
6. Elija habilitar o inhabilitar la comunicación SSL entre Management Server y el servidor LDAP.

   Nota: Puede habilitar o inhabilitar individualmente la comunicación SSL entre cada servidor y el servidor LDAP. En este caso, está estableciendo la comunicación SSL entre Management Server (IVMgr) y el servidor LDAP.
7. Si ha inhabilitado la comunicación SSL, vaya al paso 8. Si ha habilitado la comunicación SSL, especifique valores para los siguientes indicadores:
   - Ubicación del archivo de anillo de claves SSL
   - Etiqueta de la clave SSL
   - Contraseña para la clave SSL
8. Habilite el acceso a la base de datos GSO especificando el DN para el sufijo de la base de datos GSO, que ha añadido en el apartado “Añadir sufijos” en la página 24.

   Por ejemplo:

   ```
   o=IBM,c=US
   ```

Una vez que se ha configurado el acceso a la base de datos GSO, Policy Director Configuration Manager configura automáticamente un Directory Services Broker. Una serie de mensajes lista cada paso automatizado a medida que se van completando.

Aparece un mensaje que indica que la instalación del paquete IVMgr se ha realizado satisfactoriamente.

Vuelve a aparecer la lista de paquetes disponibles.

Configuración y arranque de Management Console

Para configurar Management Console, pulse el botón en **Policy Director Management Console** en la lista de configuración de Policy Director.

La configuración de Policy Director Management Console finaliza sin ninguna entrada de usuario.

Para iniciar la versión de AIX de Management Console:

1. Asegúrese de que los servidores de Policy Director están instalados y ejecutándose.
2. Escriba el siguiente mandato:

```
$ /opt/intraverse/bin/ivconsole
```

O bien, si utiliza la versión del cliente de Windows de Management Console, siga las instrucciones del apartado “Cómo iniciar Management Console” en la página 44.

Configuración de Security Manager

Para configurar Security Manager (IVNet):

1. Pulse el botón en **Policy Director Security Manager** en la lista de configuración de Policy Director.

   Aparece una serie de indicadores para integrar Security Manager con el servidor LDAP.
2. Si se le solicita, escriba la información necesaria para la configuración del servidor LDAP:
   - Nombre del sistema principal del servidor LDAP
   - Número de puerta del servidor LDAP
   - Número de puerta SSL del servidor LDAP (opcional)

   Estos indicadores no aparecen cuando Policy Director Management Server, o Authorization Server, se han configurado previamente.
3. Escriba el nombre de usuario y la contraseña del usuario administrativo de LDAP. La información de seguridad de Policy Director ahora se registra con el servidor LDAP.
4. Elija habilitar o inhabilitar la comunicación SSL entre Security Manager y el servidor LDAP.

   Nota: Puede habilitar o inhabilitar individualmente la comunicación SSL entre cada servidor de Policy Director y el servidor LDAP. En este caso, está estableciendo la comunicación SSL entre Security Manager (IVNet, para ser utilizado por WebSEAL y NetSEAL) y el servidor LDAP.

5. Si ha inhabilitado la comunicación SSL, vaya al paso 6 en la página 52. Si ha habilitado la comunicación SSL, especifique valores para los siguientes indicadores:
   - Ubicación del archivo de anillo de claves SSL
   - Etiqueta de la clave SSL
   - Contraseña para la clave SSL
6. Habilite el acceso a la base de datos GSO especificando el DN para el sufijo de la base de datos GSO, que ha añadido en el apartado "Añadir sufijos" en la página 24.

   Por ejemplo:

   ```
   o=IBM,c=US
   ```

   Este indicador no aparece cuando Policy Director Management Server, o Authorization Server, se han configurado previamente.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
7. Cuando se le indique, escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   Security Manager se configura y se inicia. El servidor CAS también se inicia.

   Aparece un mensaje que indica que la instalación del paquete Security Manager se ha realizado satisfactoriamente.

Configuración de Policy Director WebSEAL

Para configurar Policy Director WebSEAL (IVWeb):

1. Pulse el botón en **Policy Director WebSEAL** en la lista de configuración de Policy Director.

   Aparece el menú de configuración de Policy Director WebSEAL con valores que confirman lo siguiente:
   - Acceso a los clientes HTTP y HTTPS
   - Puertas TCP (Transmission Control Protocol) necesarias
   - El directorio root del documento de la Web por omisión
2. Confirme los valores de configuración actuales:

   ```
   Please check Web Server configuration:
   1. Enable TCP HTTP?                        Yes
   2. HTTP Port                              80
   3. Enable HTTPS?                              Yes
   4. HTTPS Port                            443
   5. Web document root directory        /opt/Policy Director/www/docs
   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```
3. Escriba la letra a para aceptar la configuración y seguir con la instalación, o bien especifique el número de un valor que quiera cambiar.

   La configuración de Policy Director Security Manager solicita el nombre y la contraseña del administrador de célula DCE.
4. Escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   Policy Director Security Manager se reinicia.

La instalación configura y habilita Policy Director WebSEAL en el sistema.

Configuración de Policy Director Authorization Server

Para configurar Policy Director Authorization Server (IVAcld):

1. Pulse el botón en **Policy Director Authorization Server** en la lista de configuración de Policy Director.

   Aparece uno o más indicadores para integrar Policy Director Authorization Server con el servidor LDAP.
2. Si se le solicita, escriba la información necesaria para la configuración del servidor LDAP:
   - Nombre del sistema principal del servidor LDAP
   - Número de puerta del servidor LDAP
   - Número de puerta SSL del servidor LDAP (opcional)

   Estos indicadores no aparecen cuando Policy Director Management Server, o Authorization Server, se han configurado previamente.
3. Escriba el nombre de usuario y la contraseña del usuario administrativo de LDAP. La información de seguridad de Policy Director ahora se registra con el servidor LDAP.
4. Elija habilitar o inhabilitar la comunicación SSL entre Security Manager y el servidor LDAP.

   Nota: Puede habilitar o inhabilitar individualmente la comunicación SSL entre cada servidor de Policy Director y el servidor LDAP. En este caso, está estableciendo la comunicación SSL entre Authorization Server (IVAcld) y el servidor LDAP.
5. Si ha inhabilitado la comunicación SSL, vaya al paso 6. Si ha habilitado la comunicación SSL, especifique valores para los siguientes indicadores:
   - Ubicación del archivo de anillo de claves SSL
   - Etiqueta de la clave SSL
   - Contraseña para la clave SSL
6. Habilite el acceso a la base de datos GSO especificando el DN para el sufijo de la base de datos GSO, que ha añadido en el apartado “Añadir sufijos” en la página 24.

   Por ejemplo:

   ```
   o=IBM,c=US
   ```

   Este indicador no aparece cuando Policy Director Management Server, o Authorization Server, se han configurado previamente.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
7. Cuando se le indique, escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   Authorization Server se configura y se inicia.

   Aparece un mensaje que indica que la instalación del paquete Authorization Server se ha realizado satisfactoriamente.

Configuración de Policy Director NetSEAL

Para configurar Policy Director NetSEAL:

1. Pulse el botón en **Policy Director NetSEAL** en la lista de configuración de Policy Director.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba el nombre de usuario y la contraseña del usuario administrativo de LDAP. La información de seguridad de Policy Director ahora se registra con el servidor LDAP.

   La configuración del paquete Policy Director NetSEAL ha finalizado.

Policy Director NetSEAL detecta las solicitudes que se realizan en puertas específicas. Para utilizar la detección de NetSEAL, debe parar y reiniciar todas las aplicaciones que utilizan las puertas especificadas. Para obtener más información sobre cómo utilizar Policy Director NetSEAL, consulte el apartado "Utilización de la detección de NetSEAL en AIX" en la página 58.

Configuración de Policy Director Authorization ADK

Para configurar Policy Director Authorization ADK, pulse el botón en **Policy Director Authorization ADK** en la lista de configuración de Policy Director.

La configuración del paquete Policy Director Authorization finaliza sin ninguna entrada de usuario.

Configuración de Policy Director Credentials Acquisition Service

Policy Director CAS se instala automáticamente. Si desea utilizar Policy Director CAS para su servicio de adquisición de credenciales, debe configurarlo. Puede obtener información sobre Policy Director CAS y cómo configurarlo para el servidor WebSEAL en la publicación *Policy Director Guía de administración*.

Configuración de Policy Director con un registro de usuarios DCE

Debe instalar los paquetes de software de Policy Director antes de configurarlos. Si todavía no ha instalado los paquetes de Policy Director, consulte antes el apartado "Instalación de Policy Director" en la página 47.

Si ha instalado Policy Director con un registro de usuarios LDAP, vaya al apartado "Configuración de Policy Director con un registro de usuarios LDAP" en la página 49.

Debe configurar cada paquete instalado de Policy Director, con la excepción de SMIT Setup. Configure los paquetes de uno en uno. Algunos de los paquetes de Policy Director requieren que el administrador responda a solicitudes de la pantalla durante la configuración.

Para configurar los paquetes de Policy Director:

1. Inicie la SMIT.

   Aparece el menú Gestión del sistema.
2. Pulse el botón en **Aplicaciones y servicios de comunicaciones**.

Aparece una lista de paquetes de software instalados. Por ejemplo:

- TCP/IP
- NFS
- DCE (Distributed Computing Environment)
- Policy Director

3. Pulse el botón en **Policy Director**.

   Aparece el menú Policy Director con las siguientes opciones:

   - Configuración de Policy Director
   - Desconfiguración de Policy Director

4. Pulse el botón en **Configuración de Policy Director**.

   Aparece una lista de paquetes de Policy Director instalados, como por ejemplo:

   - Configuración de Policy Director Base
   - Configuración de Policy Director Management Server
   - Configuración de Policy Director Management Console
   - Configuración de Policy Director Security Manager
   - Configuración de Policy Director WebSEAL
   - Configuración de Policy Director Authorization Server
   - Configuración de Policy Director NetSEAL
   - Configuración de Policy Director Authorization ADK

5. Pulse en cada paquete que quiera configurar, de uno en uno.

   Debe configurar los paquetes de Policy Director en el orden en que aparecen en la lista de configuración de Policy Director. Seleccione cada paquete de uno en uno, desde el elemento superior al elemento inferior.

Ahora debe configurar los paquetes de Policy Director que ha seleccionado siguiendo las instrucciones de configuración pertinentes que se indican en los apartados siguientes.

Configuración del paquete Base

El paquete Base se instala en un sistema siempre que se instala cualquiera de los demás paquetes. Para configurar el paquete Base, pulse el botón en **Policy Director Base** en la lista de configuración de Policy Director.

La configuración del paquete Policy Director finaliza sin ninguna entrada de usuario.

Configuración de Management Server

Para configurar Management Server:

1. Pulse el botón en **Policy Director Management Server** en la lista de configuración de Policy Director.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.

2. Cuando se le indique, escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   La instalación configura e inicia Management Server.

Configuración y arranque de Management Console

Para configurar Management Console, pulse el botón en **Policy Director Management Console** en la lista de configuración de Policy Director.

La configuración de Policy Director Management Console finaliza sin ninguna entrada de usuario.

Para iniciar la versión de AIX de Management Console:

1. Asegúrese de que los servidores de Policy Director están instalados y ejecutándose.
2. Escriba el siguiente mandato:

```
$ /opt/intraverse/bin/ivconsole
```

Configuración de Security Manager

Para configurar Security Manager (IVNet):

1. Pulse el botón en **Policy Director Security Manager** en la lista de configuración de Policy Director.
2. Cuando se le indique, escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

La instalación configura e inicia Security Manager.

Configuración de Policy Director WebSEAL

Para configurar Policy Director WebSEAL (IVWeb):

1. Pulse el botón en **Policy Director WebSEAL** en la lista de configuración de Policy Director.

   Aparece el menú de configuración de Policy Director WebSEAL con valores que confirman lo siguiente:

   - Acceso a los clientes HTTP y HTTPS
   - Puertas TCP (Transmission Control Protocol) necesarias
   - El directorio root del documento de la Web por omisión
2. Confirme los valores de configuración actuales:

   ```
   Please check Web Server configuration:
   1. Enable TCP HTTP?                      Yes
   2. HTTP Port                            80
   3. Enable HTTPS?                            Yes
   4. HTTPS Port                          443
   5. Web document root directory       /opt/Policy Director/www/docs
   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```
3. Escriba la letra a para aceptar la configuración y seguir con la instalación, o bien especifique el número de un valor que quiera cambiar.

   La configuración de Policy Director Security Manager solicita el nombre y la contraseña del administrador de célula DCE.
4. Escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   Policy Director Security Manager se reinicia.

La instalación configura y habilita Policy Director WebSEAL en el sistema.

Configuración de Policy Director Authorization Server

Para configurar Policy Director Authorization Server (IVAcld):

1. Pulse el botón en **Policy Director Authorization Server** en la lista de configuración de Policy Director.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba el nombre de cuenta y la contraseña del administrador de célula DCE.

   Authorization Server se configura y se inicia.

Configuración de Policy Director NetSEAL

Para configurar Policy Director NetSEAL:

1. Pulse el botón en **Policy Director NetSEAL** en la lista de configuración de Policy Director.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba el nombre de usuario y la contraseña del usuario administrativo de LDAP. La información de seguridad de Policy Director ahora se registra con el servidor LDAP.

   La configuración de Policy Director NetSEAL ha finalizado.

Policy Director NetSEAL detecta las solicitudes que se realizan en puertas específicas. Para utilizar la detección de NetSEAL, debe parar y reiniciar todas las aplicaciones que utilizan las puertas especificadas. Para obtener más información sobre cómo utilizar Policy Director NetSEAL, consulte el apartado “Utilización de la detección de NetSEAL en AIX” en la página 58.

Configuración de Policy Director Authorization ADK

Para configurar el Policy Director Authorization ADK, pulse el botón en **Policy Director Authorization ADK** en la lista de configuración de Policy Director.

La configuración del paquete Policy Director Authorization finaliza sin ninguna entrada de usuario.

Configuración de Policy Director Credentials Acquisition Service

Policy Director CAS se instala automáticamente. Si desea utilizar Policy Director CAS para su servicio de adquisición de credenciales, debe configurarlo. Puede obtener información sobre Policy Director CAS y cómo configurarlo para el servidor WebSEAL en la publicación *Policy Director Guía de administración*.

Instalación de Management Console

Policy Director proporciona una Management Console que gestiona muchos componentes del sistema de seguridad de Policy Director desde un escritorio de

cliente de Windows. Management Console puede instalarse en cualquiera de los siguientes sistemas operativos:

- Windows 95
- Windows 98
- Windows NT Versión 4.0, con Service Pack 4 o superior
- AIX Versión 4.3.1.0 o superior

Cada sistema operativo de Windows que ejecute Policy Director requiere el cliente Policy Director NetSEAT.

El cliente NetSEAT puede configurarse como un cliente de ejecución DCE o como un cliente para un servidor de Policy Director. Aunque cualquiera de las dos configuraciones anteriores es aceptable para Management Console, los servidores de Policy Director requieren todo el cliente para el servidor de Policy Director.

Si necesita reinstalar algún componente, debe eliminar el componente existente antes de reinstalarlo.

Utilización de la detección de NetSEAL en AIX

Para utilizar la detección de Policy Director NetSEAL, es necesario iniciar el daemon de NetSEAL Security Manager (secmgrd) antes que las aplicaciones que acceden a las puertas protegidas (detectadas). Utilice las entradas /etc/inittab para asegurarse de que secmgrd se inicia antes que las aplicaciones durante el proceso de arranque.

Utilice la detección de NetSEAL con aplicaciones de redes, como por ejemplo Telnet, RLOGIN y POP3. El daemon **inetd** controla dichas aplicaciones. El script de arranque de Policy Director, /etc/iv/iv, inicia secmgrd, y luego se para y reinicia el daemon inetd. Este procedimiento asegura la inclusión satisfactoria de estas aplicaciones después de arrancar el sistema.

Si para y reinicia Policy Director, también debe parar y reiniciar todas las aplicaciones que realizan solicitudes a puertas detectadas. Para automatizar este proceso, puede añadir código a /etc/iv/iv para parar e iniciar las aplicaciones después de que se inicie secmgrd. Utilice la técnica del script /etc/iv/iv para parar y reiniciar **inetd** como plantilla para parar e iniciar otras aplicaciones.

Para obtener más información sobre cómo configurar Policy Director NetSEAL para detectar puertas específicas, consulte la información sobre NetSEAL en la publicación *Policy Director Guía de administración*.

Eliminación de Policy Director

Debe desconfigurar Policy Director para AIX antes de eliminarlo.

- Para obtener información sobre cómo desconfigurar Policy Director, consulte el apartado “Desconfiguración de paquetes de Policy Director” en la página 59.
- Para obtener información sobre cómo eliminar Policy Director, consulte el apartado “Eliminación de paquetes de Policy Director” en la página 59.

Para eliminar la versión Windows de Management Console, consulte

Desconfiguración de paquetes de Policy Director

Para desconfigurar los servidores de Policy Director, lleve a cabo los siguientes pasos:

1. Inicie la SMIT.
2. Pulse el botón en **Aplicaciones y servicios de comunicaciones**.

   Aparece el menú Aplicaciones y servicios de comunicaciones.
3. Pulse el botón en **Policy Director**.

   Aparece el menú Policy Director.
4. En dicho menú, pulse el botón en **Desconfiguración de Policy Director**.

   Aparece la lista de paquetes de Policy Director configurados.

   Seleccione el paquete que desea desconfigurar. Los paquetes que pueden aparecer son los siguientes:
   - Desconfiguración de Policy Director Authorization Server
   - Desconfiguración de Policy Director Authorization ADK
   - Desconfiguración de Policy Director NetSEAL
   - Desconfiguración de Policy Director WebSEAL
   - Desconfiguración de Policy Director Security Manager
   - Desconfiguración de Policy Director Management Server
   - Desconfiguración de Policy Director Management Console
   - Desconfiguración de Policy Director Base
   - Desconfiguración del menú de IV Smit
5. Los paquetes deben desconfigurarse de uno en uno.

   Nota: Debe desconfigurar los paquetes en el orden inverso en el que se han instalado. Para seguir este orden, desconfigure los paquetes desde la parte superior del menú hasta la parte inferior del mismo.

6. Si está desconfigurando los paquetes de Policy Director porque desea eliminar la totalidad de Policy Director del sistema, pulse el botón en **Desconfiguración del menú Policy Director Smit** después de desconfigurar los demás paquetes de Policy Director.

   Este paso elimina la información sobre los paquetes de Policy Director de la base de datos de la SMIT.
7. Consulte el apartado “Eliminación de paquetes de Policy Director” para eliminar Policy Director.

Eliminación de paquetes de Policy Director

Antes de intentar eliminar Policy Director, verifique antes que el software de Policy Director se ha desconfigurado. El apartado “Desconfiguración de paquetes de Policy Director” ofrece instrucciones para la desconfiguración.

Para eliminar Policy Director:

1. Inicie la SMIT.
2. Pulse el botón en **Instalación y mantenimiento de software**.

   Aparece el menú Instalación y mantenimiento de software.

3. Pulse el botón en **Mantenimiento de software y programas de utilidad**.

   Aparece el menú Mantenimiento de software y programas de utilidad.
4. Pulse el botón en **Eliminar software instalado**.

   Aparece la ventana Eliminar software instalado.
5. Seleccione los paquetes de Policy Director que desea eliminar. Puede seleccionar más de un paquete a la vez.

   Para eliminar todos los paquetes de Policy Director, escriba `IV`.

El software de Policy Director se elimina.

Eliminación de Management Console y NetSEAT

Management Console de Windows y el cliente NetSEAT de Windows pueden eliminarse utilizando la función de desinstalación InstallShield.

- Elimine Management Console. Consulte el apartado “Eliminación de Management Console” en la página 44 para ver las instrucciones.
- Elimine el cliente NetSEAT. Consulte el apartado “Eliminación del cliente NetSEAT” en la página 45 para ver las instrucciones.

Capítulo 7. Instalación de Policy Director para Solaris

Los apartados de este capítulo explican cómo instalar y configurar Policy Director en el sistema operativo Solaris.

Antes de empezar la instalación de Policy Director, revise la información del apartado “Antes de instalar Policy Director para Solaris”.

Antes de instalar Policy Director para Solaris

Antes de empezar la instalación de Policy Director, lea la siguiente información:

El procedimiento de instalación de este release de Policy Director requiere el mandato **pkgadd**. Para ejecutar el mandato **pkgadd**, escriba lo siguiente en la línea de mandatos:

```
# pkgadd -d /cdrom/cdrom0/solaris
```

Utilice el mandato **pkgadd** para instalar el software de Policy Director. El mandato **pkgadd** a menudo muestra solicitudes complementarias que no se indican en las instrucciones del procedimiento estándar. Estas solicitudes aparecen como respuesta a situaciones específicas a la instalación y configuración de su sistema. Responda siempre y a estas solicitudes que se producen fuera del procedimiento estándar.

Antes de instalar Policy Director:

- Debe instalar un cliente DCE.
- Si utiliza LDAP para su registro de usuarios, también debe instalar un cliente LDAP.

Debe habilitar las funciones de administración remota de Transarc DCE antes de empezar la instalación de Policy Director. No podrá llevar a cabo la instalación de Policy Director si las funciones de administración remota no están habilitadas.

La utilización de algunas funciones de administración remota permite que el administrador de célula pueda llegar a ser esencialmente equivalente a la cuenta root local. Transarc DCE normalmente inhabilita estas funciones de administración remota. Sin embargo, el software de Policy Director necesita dichas funciones.

Consulte el apartado 4.2.1 de la publicación *Transarc Release Notes, Release 1.1* (DCE-D1002-01) para obtener información sobre cómo habilitar las funciones de administración remota.

Salida de pantalla de instalación

Los procedimientos estándares de este documento no indican todas las salidas de pantalla posibles con el mandato **pkgadd**. La mayoría de las salidas de pantalla no documentadas proporcionan información adicional sobre las operaciones que se están realizando. En general, los procedimientos estándares contenidos en esta documentación sólo muestran aquellos mensajes que requieren una respuesta por parte del usuario.

Instalación de servidores de Policy Director con un registro de usuarios LDAP

Si instala Policy Director con un registro de usuarios DCE, vaya al apartado “Instalación del servidor de Policy Director con un registro de usuarios DCE” en la página 67.

Los paquetes de los servidores se encuentran en el directorio /solaris del CD *IBM SecureWay Policy Director Versión 3.0*.

Debe estar conectado como usuario root para instalar los paquetes de Policy Director.

Si debe reinstalar algún paquete, primero debe eliminar el paquete existente (**pkgrm**) antes de reinstalar el paquete deseado.

Para instalar Management Server:

1. Asegúrese de que el servidor LDAP está instalado y ejecutándose si va a utilizar LDAP como registro de usuarios. Consulte el Capítulo 4, “Instalación y configuración de IBM SecureWay Directory” en la página 23 para ver las instrucciones completas.
2. Escriba el mandato **pkgadd** para ver una lista de los paquetes disponibles en el CD:

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   La lista de paquetes disponibles aparece en pantalla.

   Si utiliza un punto de montaje distinto del CD-ROM, sustitúyalo en el mandato anterior.
3. Escriba el número de selección de IVBase para instalar los archivos de Policy Director Base y luego pulse Intro.

   Este mandato extrae los archivos del CD y los instala en la ubicación que especifique del disco duro.

   Aparece un indicador informando que la instalación del paquete IVBase se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

   Antes de continuar con el siguiente paso, recuerde que sólo debe haber una instancia de Management Server (IVMgr) en el dominio seguro. Si se trata de una instalación en un sistema autónomo, continúe con el paso siguiente. Si está instalando en un servidor secundario, revise el apartado “Requisitos de instalación para el dominio seguro” en la página 18.
4. Escriba el número de selección de IVMgr para instalar los archivos de Policy Director Management Server. Pulse Intro.

   Este mandato extrae los archivos del CD y los instala en la ubicación que especifique del disco duro.

   Aparece un indicador que le solicita que elija un tipo de registro de usuarios.
5. Si utiliza LDAP para su registro de usuarios, escriba 2 para el registro de usuarios LDAP.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
6. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

```
Especifique el nombre de usuario del administrador de célula [cell_admin]:
Especifique la contraseña para el administrador de célula:
```

Aparece una serie de indicadores para configurar la comunicación entre Management Server y el servidor LDAP.

7. Escriba la información necesaria para la configuración del servidor LDAP:
   - Nombre del sistema principal del servidor LDAP
   - Número de puerta del servidor LDAP
   - Número de puerta SSL del servidor LDAP
8. Escriba el DN y la contraseña del usuario administrativo de LDAP (por ejemplo, `cn=root`). El servidor LDAP ahora contiene la información de seguridad de Policy Director.
9. Elija habilitar o inhabilitar la comunicación SSL entre Management Server y el servidor LDAP.

   Puede habilitar o inhabilitar individualmente la comunicación SSL entre cada servidor de Policy Director y el servidor LDAP. En este caso, está estableciendo la comunicación SSL entre Management Server y el servidor LDAP.
10. Si ha inhabilitado la comunicación SSL, sáltese este paso. Si ha habilitado la comunicación SSL, especifique valores para los siguientes indicadores:
    - `Ubicación del archivo de anillo de claves SSL`
    - `Etiqueta de la clave SSL`
    - `Contraseña para la clave SSL`
11. Habilite el acceso a la base de datos GSO especificando el DN para el sufijo de la base de datos GSO, que ha añadido en el apartado “Añadir sufijos” en la página 24.

    Por ejemplo:

    ```
    o=IBM,c=US
    ```

    Una vez que se ha configurado el acceso a la base de datos GSO, Policy Director Configuration Manager configura automáticamente un DSB. Una serie de mensajes lista cada paso automatizado a medida que se van completando.

    Aparece un mensaje que indica que la instalación del paquete IVMgr se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Instalación de Security Manager para WebSEAL y NetSEAL

El paquete Security Manager (IVNet) necesita recursos del paquete Base. Asegúrese de que el componente Base está instalado antes de instalar IVNet.

1. Escriba el número de selección de IVNet para instalar los archivos de Policy Director Security Manager y luego pulse Intro.

   Los archivos se extraen del CD y se instalan en el disco duro en el directorio por omisión.

   Si utiliza LDAP como su registro de usuarios, aparece una serie de indicadores para integrar Security Manager con el servidor LDAP.
2. Si se le solicita, escriba la información necesaria para la configuración del servidor LDAP:
   - Nombre del sistema principal del servidor LDAP
   - Número de puerta del servidor LDAP

- Número de puerta SSL del servidor LDAP

Los indicadores anteriores para la configuración del servidor LDAP sólo aparecen si la comunicación con el servidor LDAP no se ha configurado previamente para ningún otro paquete de Policy Director de este sistema. Si Management Server (IVMgr) o Authorization Server (IVAcld) se han configurado en este sistema, los indicadores anteriores no aparecen en este paso.

3. Escriba el DN y la contraseña del usuario administrativo de LDAP.

   El servidor LDAP ahora contiene la información de seguridad de Policy Director.

4. Elija habilitar o inhabilitar la comunicación SSL entre Security Manager y el servidor LDAP.

   Puede habilitar o inhabilitar individualmente la comunicación SSL entre cada servidor de Policy Director y el servidor LDAP. En este caso, está estableciendo la comunicación SSL entre Security Manager y el servidor LDAP.

5. Si ha inhabilitado la comunicación SSL, sáltese este paso. Si ha habilitado la comunicación SSL, especifique valores para los siguientes indicadores:
   - `Ubicación del archivo de anillo de claves SSL`
   - `Etiqueta de la clave SSL`
   - `Contraseña para la clave SSL`

6. Habilite el acceso a la base de datos GSO especificando el DN para el sufijo de la base de datos GSO, que ha añadido en el apartado “Añadir sufijos” en la página 24.

   Por ejemplo:

   ```
   o=IBM,c=US
   ```

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.

7. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   ```
   Escriba el nombre de usuario del administrador de célula [admin_cél]:
   Escriba la contraseña para el administrador de célula:
   ```

   Security Manager se configura y se inicia.

   El servidor CAS se configura y se inicia.

   Aparece un indicador informando que la instalación del paquete IVNet se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Habilitación del componente WebSEAL

Instale el paquete WebSEAL (IVWeb) si desea habilitar el componente WebSEAL.

1. Escriba el número de selección de IVWeb para instalar los archivos necesarios para habilitar el componente del servidor HTTP de WebSEAL.
2. Pulse Intro para continuar.

   Los archivos se extraen del CD y se instalan en el disco duro.

   Aparece una lista de configuración con valores que confirman el acceso a los clientes HTTP y HTTPS, las puertas TCP necesarias y el directorio root del documento de la Web por omisión.

3. Confirme los valores de configuración actuales:

```
Check Web Server configuration:
1. Enable TCP HTTP?     Yes
2. HTTP Port    80
3. Enable HTTPS?        Yes
4. HTTPS Port   443
5. Web document root directory /opt/Policy Director/www/docs

a. Accept configuration and continue with installation
x. Exit installation

Select item to change: a
```

4. Escriba la letra a para aceptar la configuración y seguir con la instalación, y luego pulse Intro.
5. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

```
Escriba el nombre de usuario del administrador de célula [cell_admin]:
Escriba la contraseña para el administrador de célula:
```

   La instalación configura y habilita WebSEAL en el sistema. Security Manager se reinicia automáticamente.

Habilitación del componente NetSEAL

Instale el paquete NetSEAL (IVTrap) si desea habilitar el componente NetSEAL.

1. Escriba el número de selección de IVTrap para instalar los archivos necesarios para habilitar el componente de control de accesos flexible TCP/IP de NetSEAL y luego pulse Intro.

   NetSEAL se configura y se habilita.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   Aparece un mensaje indicándole que debe especificar las puertas protegidas utilizando el mandato **ivadmin**.

   Aparece otro mensaje que le indica que debe reiniciar (rearrancar) el sistema para asegurarse de que todas las puertas protegidas están colocadas bajo el control de NetSEAL.

   Aparece un indicador informando que la instalación del paquete IVTrap se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Policy Director NetSEAL detecta las solicitudes que se realizan en puertas específicas. Para utilizar la detección de NetSEAL, debe parar y reiniciar todas las aplicaciones que utilizan las puertas especificadas. Para obtener más información sobre cómo configurar Policy Director NetSEAL, consulte la información general de NetSEAL en la publicación *Policy Director Guía de administración*.

Instalación de Authorization Server

Para instalar Authorization Server:

1. Escriba el número de selección de IVAcld para instalar los archivos de Policy Director Authorization Server y luego pulse Intro.

Los archivos se extraen del CD y se instalan en el disco duro en el directorio por omisión.

Si utiliza LDAP como su registro de usuarios, aparece una serie de indicadores para integrar Authorization Server con el servidor LDAP.

2. Si se le solicita, escriba la información necesaria para la configuración del servidor LDAP:
   - Nombre del sistema principal del servidor LDAP
   - Número de puerta del servidor LDAP
   - Número de puerta SSL del servidor LDAP

   Los indicadores anteriores para la configuración del servidor LDAP sólo aparecen si la comunicación con el servidor LDAP no se ha configurado previamente para ningún otro paquete de Policy Director de este sistema. Si Management Server (IVMgr) o Security Manager (IVNet) se han configurado en este sistema, los indicadores anteriores no aparecen en este paso.
3. Escriba el DN y la contraseña del usuario administrativo de LDAP.

   El servidor LDAP ahora contiene la información de seguridad de Policy Director.
4. Elija habilitar o inhabilitar la comunicación SSL entre Management Server y el servidor LDAP.

   Puede habilitar o inhabilitar individualmente la comunicación SSL entre cada servidor de Policy Director y el servidor LDAP. En este caso, está estableciendo la comunicación SSL entre Management Server y el servidor LDAP.
5. Si ha inhabilitado la comunicación SSL, sáltese este paso. Si ha habilitado la comunicación SSL, especifique valores para los siguientes indicadores:
   - `Ubicación del archivo de anillo de claves SSL`
   - `Etiqueta de la clave SSL`
   - `Contraseña para la clave SSL`
6. Habilite el acceso a la base de datos GSO especificando el DN para el sufijo de la base de datos GSO, que ha añadido en el apartado “Añadir sufijos” en la página 24.

   Por ejemplo:

   ```
   o=IBM,c=US
   ```

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
7. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   ```
   Escriba el nombre de usuario del administrador de célula [cell_admin]:
   Escriba la contraseña para el administrador de célula:
   ```

   Authorization Server se configura y se inicia.

   Aparece un indicador informando que la instalación del paquete IVAcld se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Instalación del componente API de autorizaciones

Para instalar la API de autorizaciones para archivos en C, escriba el número de selección de IVAuthADK y luego pulse Intro.

Los archivos se extraen del CD y se instalan en el disco duro en el directorio por omisión.

Aparece un indicador informando que la instalación del paquete IVAuthADK se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Instalación del servidor de Policy Director con un registro de usuarios DCE

Si instala Policy Director con un registro de usuarios LDAP, vaya al apartado "Instalación de servidores de Policy Director con un registro de usuarios LDAP" en la página 62.

Los paquetes de los servidores se encuentran en el directorio /solaris del CD *IBM SecureWay Policy Director Versión 3.0*.

Debe estar conectado como usuario root para instalar los paquetes de Policy Director.

Si debe reinstalar algún paquete, primero debe eliminar el paquete existente (**pkgrm**) antes de reinstalar el paquete deseado.

Para instalar Management Server:

1. Escriba el mandato **pkgadd** para ver una lista de los paquetes disponibles en el CD:

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   La lista de paquetes disponibles aparece en pantalla.

   Si utiliza un punto de montaje distinto del CD-ROM, sustitúyalo en el mandato anterior.
2. Escriba el número de selección de IVBase para instalar los archivos de Policy Director Base y luego pulse Intro.

   Este mandato extrae los archivos del CD y los instala en la ubicación que especifique del disco duro.

   Aparece un indicador informando que la instalación del paquete IVBase se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

   Antes de continuar con el siguiente paso, recuerde que sólo debe haber una instancia de Management Server (IVMgr) en el dominio seguro. Si se trata de una instalación en un sistema autónomo, continúe con el paso siguiente. Si está instalando en un servidor secundario, revise el apartado "Requisitos de instalación para el dominio seguro" en la página 18.
3. Escriba el número de selección de IVMgr para instalar los archivos de Policy Director Management Server. Pulse Intro.

   Este mandato extrae los archivos del CD y los instala en la ubicación que especifique del disco duro.

   Aparece un indicador que le solicita que elija un tipo de registro de usuarios.
4. Si utiliza DCE para su registro de usuarios, escriba 1.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.

5. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   ```
   Especifique el nombre de usuario del administrador de célula [cell_admin]:
   Especifique la contraseña para el administrador de célula:
   ```

   Aparece un mensaje que indica que la instalación del paquete IVMgr se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Instalación de Security Manager para WebSEAL y NetSEAL

El paquete Security Manager (IVNet) necesita recursos del paquete Base. Asegúrese de que el componente Base está instalado antes de instalar IVNet.

1. Escriba el número de selección de IVNet para instalar los archivos de Policy Director Security Manager y luego pulse Intro.

   Los archivos se extraen del CD y se instalan en el disco duro en el directorio por omisión. Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   ```
   Escriba el nombre de usuario del administrador de célula
   [cell_admin]:
   Escriba la contraseña para el administrador de célula:
   ```

   Security Manager se configura y se inicia.

   Aparece un indicador informando que la instalación del paquete IVNet se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Habilitación del componente WebSEAL

Instale el paquete WebSEAL (IVWeb) si desea habilitar el componente WebSEAL.

1. Escriba el número de selección de IVWeb para instalar los archivos necesarios para habilitar el componente del servidor HTTP de WebSEAL.
2. Pulse Intro para continuar.

   Los archivos se extraen del CD y se instalan en el disco duro.

   Aparece una lista de configuración con valores que confirman el acceso a los clientes HTTP y HTTPS, las puertas TCP necesarias y el directorio root del documento de la Web por omisión.
3. Confirme los valores de configuración actuales:

   ```
   Check Web Server configuration:
   1. Enable TCP HTTP?     Yes
   2. HTTP Port    80
   3. Enable HTTPS?        Yes
   4. HTTPS Port   443
   5. Web document root directory /opt/Policy Director/www/docs

   a. Accept configuration and continue with installation
   x. Exit installation

   Select item to change: a
   ```

4. Escriba la letra a para aceptar la configuración y seguir con la instalación, y luego pulse Intro.

5. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   ```
   Escriba el nombre de usuario del administrador de célula
   [cell_admin]:
   Escriba la contraseña para el administrador de célula:
   ```

   La instalación configura y habilita WebSEAL en el sistema. Security Manager se reinicia automáticamente.

Habilitación del componente NetSEAL

Instale el paquete NetSEAL (IVTrap) si desea habilitar el componente NetSEAL.

1. Escriba el número de selección de IVTrap para instalar los archivos necesarios para habilitar el componente de control de accesos flexible TCP/IP de NetSEAL y luego pulse Intro.

   NetSEAL se configura y se habilita.

   Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   Aparece un mensaje indicándole que debe especificar las puertas protegidas utilizando el mandato **ivadmin**.

   Aparece otro mensaje que le indica que debe reiniciar (rearrancar) el sistema para asegurarse de que todas las puertas protegidas están colocadas bajo el control de NetSEAL.

   Aparece un indicador informando que la instalación del paquete IVTrap se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Policy Director NetSEAL detecta las solicitudes que se realizan en puertas específicas. Para utilizar la detección de NetSEAL, debe parar y reiniciar todas las aplicaciones que utilizan las puertas especificadas. Para obtener más información sobre cómo configurar Policy Director NetSEAL, consulte la información general de NetSEAL en la publicación *Policy Director Guía de administración.*

Instalación de Authorization Server

Para instalar Authorization Server:

1. Escriba el número de selección de IVAcld para instalar los archivos de Policy Director Authorization Server y luego pulse Intro.

   Los archivos se extraen del CD y se instalan en el disco duro en el directorio por omisión. Aparece un indicador solicitándole el nombre y la contraseña del administrador de célula DCE.
2. Escriba la información necesaria para acceder a la cuenta del administrador de célula DCE.

   ```
   Escriba el nombre de usuario del administrador de célula [cell_admin]:
   Escriba la contraseña para el administrador de célula:
   ```

   Authorization Server se configura y se inicia.

   Aparece un indicador informando que la instalación del paquete IVAcld se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Instalación del componente API de autorizaciones

Para instalar la API de autorizaciones para archivos en C, escriba el número de selección de IVAuthADK y luego pulse Intro.

Los archivos se extraen del CD y se instalan en el disco duro en el directorio por omisión.

Aparece un indicador informando que la instalación del paquete IVAuthADK se ha realizado satisfactoriamente. Vuelve a aparecer la lista de paquetes disponibles.

Configuración de Credentials Acquisition Service

Policy Director CAS se instala automáticamente. Si desea utilizar Policy Director CAS para su servicio de adquisición de credenciales, debe configurarlo. Consulte la información sobre cómo configurar un servicio de adquisición de credenciales en la publicación *Policy Director Guía de administración* para obtener instrucciones.

Instalación de Management Console

Policy Director proporciona una Management Console que gestiona muchos de los componentes de Policy Director.

Management Console para Solaris se instala utilizando el paquete de instalación IVConsole. Utilice **pkgadd** para instalar y configurar el paquete.

1. Inicie la sesión como root.
2. Inserte y monte el CD *IBM SecureWay Policy Director Versión 3.0* en la unidad de CD-ROM del sistema de servidor de Policy Director.
3. Visualice la lista de paquetes disponibles:

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```
4. Escriba el número de selección de IVBase si todavía no se ha instalado. Si IVBase ya se ha instalado, vaya al paso 6.
5. Escriba y para continuar.

   Aparece la lista de paquetes.
6. Escriba el número de selección para IVConsole.
7. Escriba y para continuar.

   Aparece un indicador informando que la instalación se ha realizado satisfactoriamente. Management Console ahora está lista para iniciarse.

Inicio de Management Console

Para iniciar Management Console:

1. Asegúrese de que los servidores de Policy Director están instalados y ejecutándose.
2. Escriba el siguiente mandato:

```
$ /opt/intraverse/bin/ivconsole
```

Eliminación de Policy Director

Elimine los servidores de Policy Director del sistema utilizando el programa de utilidad **pkgrm**. Los paquetes deben eliminarse en el orden opuesto al seguido durante la instalación. Los mandatos **pkgrm** y **pkgadd** son miembros de la misma familia de programas de utilidad y tienen la misma interfaz de usuario. El usuario root ejecuta el programa de utilidad **pkgrm**.

Existen varios métodos para utilizar este mandato:

- Inicie el mandato **pkgrm** sin argumentos.

  Aparece una lista numerada con los paquetes actuales que hay en el sistema. Escriba un único número de selección para el paquete que desea eliminar.
- Inicie el mandato **pkgrm** y especifique un único nombre de paquete como argumento del mandato. Por ejemplo:

  ```
  # pkgrm IVBase
  ```
- Inicie el mandato **pkgrm** y especifique una secuencia de nombres de paquetes como varios argumentos del mandato. Por ejemplo:

  ```
  # pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
  ```

Consulte la documentación del sistema operativo Solaris para obtener información más detallada sobre el mandato **pkgrm**.

Nota: Debe eliminar los paquetes de Policy Director exactamente en el orden inverso al realizado para la instalación.

Para eliminar Policy Director:

1. Inicie una sesión en el sistema operativo Solaris como root.

   Utilice uno de los métodos anteriores para iniciar el mandato **pkgrm**.
2. Los componentes de Policy Director deben eliminarse en el siguiente orden:
   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

   La configuración de su sistema podría no incluir todos los paquetes que aparecen en la lista anterior. Policy Director Management Console (IVConsole) puede eliminarse en cualquier momento antes que IVBase.

Eliminación de Management Console

Para eliminar Management Console:

1. Inicie la sesión como usuario root.
2. Escriba el siguiente mandato:

   ```
   # pkgrm ivconsole
   ```

Capítulo 8. Documentación relacionada

Puede utilizar la documentación que aparece en este capítulo para encontrar más información sobre Policy Director Versión 3.0 y productos relacionados.

Documentación de Policy Director

Este manual, *Funcionamiento y ejecución de IBM SecureWay Policy Director, Versión 3.0*, además de incluirse en el producto Policy Director, también está disponible en un paquete de documentación. El paquete de documentación de Policy Director incluye este manual y la información sobre la licencia de Policy Director.

Además de este manual, los siguientes documentos contienen información sobre Policy Director y están disponibles en formato PDF (PostScript Document Format) bajo el subdirectorio /doc en el CD *IBM SecureWay Policy Director Versión 3.0*:

- *IBM SecureWay Policy Director Guía de administración, Versión 3.0*

  Este manual incluye instrucciones detalladas para la administración de Policy Director. Este manual proporciona información sobre IBM SecureWay Policy Director e incluye temas como los siguientes:

  — Conceptos sobre Policy Director, como por ejemplo autentificación, autorización y adquisición de credenciales
  — Tareas de administración general utilizando Management Console
  — Administración de WebSEAL
  — Administración de NetSEAL
  — Administración de NetSEAT
  — Recursos de administración (el mandato **ivadmin**).
- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

  Este manual explica los componentes de la API de autorizaciones y cómo realizar las siguientes tareas:

  — Creación de aplicaciones con la API de autorizaciones
  — Inicialización del servicio de autorizaciones de Policy Director
  — Autentificación de un servidor o cliente de aplicaciones
  — Obtención de credenciales de usuario
  — Toma de decisiones para una autorización
  — Realización de tareas opcionales
  — Limpieza y cierre
  — Despliegue de aplicaciones con la API de autorizaciones

El archivo README de Policy Director puede contener información más actualizada sobre Policy Director que reemplaza las publicaciones del producto.

Para obtener el archivo README más actual, acceda a la página de bibliotecas del sitio Web de IBM SecureWay Policy Director.

`http://www.ibm.com/software/security/policy/library`

Documentación de IBM SecureWay FirstSecure

El siguiente manual contiene información sobre FirstSecure:

- *IBM SecureWay FirstSecure Planificación e integración, Versión 2.0 (S564-8D11–00)*

Este manual describe FirstSecure así como los productos de que consta y le ayudará a utilizar todos los productos de IBM SecureWay.

IBM SecureWay Policy Director (Policy Director) está disponible como un componente de IBM SecureWay FirstSecure o como un producto autónomo. Si su versión de Policy Director se incluye en la oferta de FirstSecure, este manual se suministra con FirstSecure. Si su versión de Policy Director se adquirió como producto autónomo, este manual puede encontrarse en la página Web de FirstSecure Web:

`http://www.ibm.com/software/security/firstsecure/library`

Documentación de IBM Distributed Computing Environment

Los siguientes documentos, que explican cómo instalar DCE, se encuentran en el CD de *IBM SecureWay Policy Director Security Services* en formato PDF, bajo /doc o en el sitio Web de DCE:

`http://www.ibm.com/network/dce/library/`

IBM DCE para Windows NT

IBM Distributed Computing Environment for Windows NT Quick Beginnings, Version 2.2, está disponible en la siguiente dirección:

`http://www.software.ibm.com/network/dce/library/publications/dcent.html`

Este manual describe el producto Distributed Computing Environment (DCE) para Windows NT, Versión 2.2 y explica cómo planificar, instalar y configurar el producto.

El manual *IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2* también está disponible en el CD *IBM SecureWay Policy Director Security Services* en /doc/DCE22_QuickBeginnings_NT.pdf.

IBM DCE para AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2, disponible en la siguiente dirección de la Web:

`http://www.software.ibm.com/network/dce/library/publications/dceaix.html`

Este manual describe el producto IBM Distributed Computing Environment para AIX, Versión 2.2 (DCE 2.2 para AIX) y explica cómo planificar, instalar y configurar el producto.

El manual *IBM Distributed Computing Environment for AIX Quick Beginnings Version 2.2* también está disponible en el CD *IBM SecureWay Policy Director Security Services* en /doc/DCE22_QuickBeginnings_AIX.pdf.

Transarc DCE para Solaris

Las publicaciones *Transarc DCE Version 2.0 Release Notes* y *Installation and Configuration Guide* están disponibles en la siguiente dirección de la Web:

`http://www.transarc.com/Library/documentation/dce/2.0/index.html`

La publicación *Transarc DCE Version 2.0 Release Notes* proporciona la siguiente información sobre el software y la documentación de Transarc DCE:

- Diferencias entre los productos OSF DCE y DCE * DFS.
- Diferencias entre la Versión 2.0 y la Versión 1.1 de DCE * DFS
- Limitaciones y defectos conocidos asociados con DCE * DFS

La publicación *Transarc DCE Version 2.0 Release Notes* también está disponible en el CD *IBM SecureWay Policy Director Security Services* en /doc/DCE20_ReleaseNotes_Solaris.pdf.

El manual *Installation and Configuration Guide* facilita las instrucciones para instalar, configurar y actualizar el producto DCE DFS 2.0.

El manual *Installation and Configuration Guide* también está disponible en el CD *IBM SecureWay Policy Director Security Services* en /doc/DCE20_InstallGuide_Solaris.pdf.

Documentación de IBM SecureWay Directory

El siguiente manual contiene información para la instalación y configuración de IBM SecureWay Directory (LDAP):

- *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*

  Existe una versión distinta de este manual, en formato HTML, para cada sistema operativo soportado. El manual de cada sistema operativo se encuentra en el CD correspondiente en /doc/wparent.htm. Los CD son los siguientes:

  — *IBM SecureWay Directory Versión 3.1.1 para NT*

  — *IBM SecureWay Directory Versión 3.1.1 para AIX*

  — *IBM SecureWay Directory Versión 3.1.1 para Solaris*

  Después de la instalación de LDAP, la ubicación del archivo de documentación .HTM de instalación y configuración es la siguiente:

  ```
  C:\Archivos de programa\IBM\LDAP\nls\html\enUS1252\config\wparent.htm
  ```

El siguiente manual en archivo HTML contienen información sobre cómo administrar IBM SecureWay:

- *IBM SecureWay Directory Guía de administración, Versión 3.1.1*

  1. Utilizando un navegador Web, acceda a la documentación que se encuentra en esta dirección de la Web después de una instalación por omisión de LDAP:

     ```
     C:\Archivos de programa\IBM\LDAP\nls\html\enUS1252\config\wparent.ht
     ```

El siguiente manual en formato HTML contiene información sobre el cliente de IBM SecureWay Directory:

- *IBM SecureWay Directory Client SDK Programming Reference, Version 3.1.1*

  Este manual contiene enlaces con la siguiente información sobre LDAP:

  — Información sobre LDAP Client SDK Plugin Programming Reference

  1. Utilizando un navegador Web, acceda a la documentación que se encuentra en esta dirección de la Web después de una instalación por omisión de LDAP:

     ```
     C:\Archivos
     de programa\IBM\doc\progref.htm
     ```

  2. Abra la documentación de *IBM SecureWay Directory Client SDK Programming Reference*.
  3. Pulse el botón en **Apéndices**.
  4. Pulse el botón en **LDAP Client SDK Plugin Programming Reference**

— La información sobre cómo utilizar GSKit y Key Management Tool **ikmguiw** para configurar el servidor LDAP para dar soporte al acceso SSL

1. Si este manual todavía no está abierto, abra la documentación de *IBM SecureWay Directory Client SDK Programming Reference*.
2. Pulse el botón en **Categorías de API**.
3. Pulse el botón en **SSL**.
4. Pulse el botón en **API LDAP_SSL**.
5. Busque y pulse el enlace **Utilización de IKMGUI** para abrir el archivo HTML correspondiente.

El siguiente documento también está disponible para el servidor IBM SecureWay Directory:

- *IBM SecureWay Directory Server Plug-ins Reference*

Apéndice A. Avisos

Esta información ha sido desarrollada para productos y servicios que se ofrecen en los Estados Unidos. Es posible que, en otros países, IBM no ofrezca los productos, servicios o funciones que se describen en este documento. Póngase en contacto con el representante local de IBM para que le informe sobre los productos y servicios disponibles en su área. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse los productos, programas o servicios de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que afecten a los temas tratados en este documento. La posesión de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Si desea consultar cualquier tema relacionado con información de doble byte (DBCS), póngase en contacto con el departamento IBM Intellectual Property Department de su país o envíe dichas consultas, por escrito, a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106, Japón

El siguiente párrafo no se aplica al Reino Unido ni a cualquier otro país en que dichas disposiciones contradigan la legislación vigente: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN " TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN QUE ELLO CONSTITUYA UN LÍMITE, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN FIN CONCRETO. Algunas legislaciones no contemplan la exclusión de garantías, ni implícitas ni explícitas, por lo que puede haber usuarios no afectados por esta disposición.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; dichos cambios se incorporarán en nuevas ediciones de la información. IBM se reserva el derecho de realizar, si lo considera oportuno, cualquier modificación en los productos o programas que se describen en esta información sin necesidad de notificarlo previamente.

Cualquier referencia realizada en esta publicación a sitios Web que no son de IBM se proporciona únicamente por comodidad y, de ningún modo, constituye una recomendación de dichos sitios Web. Los materiales de dichos sitios Web no forman parte de los materiales de este producto IBM y el usuario que los utilice lo hará bajo su cuenta y riesgo.

Al enviar comentarios a IBM, se concede a IBM un derecho no exclusivo de utilización o distribución de los mismos en la forma que considere adecuada y sin incurrir por ello en ninguna obligación para con el remitente.

Los titulares de licencias de este programa que deseen información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) la utilización mutua de la información intercambiada, deben ponerse en contacto con:

IBM S.A.
National Language Support
Diagonal 571
08029 Barcelona
España

Dicha información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo, en algunos casos, el pago de unos derechos.

El programa bajo licencia descrito en este documento y todo el material bajo licencia del que dispone lo proporciona IBM en los términos del Acuerdo de Cliente IBM, Acuerdo de Licencia de Programación Internacional de IBM o cualquier otro acuerdo equivalente entre IBM y el usuario.

Los datos sobre rendimiento que contiene este documento se determinaron en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos pueden variar significativamente. Determinadas mediciones pueden haberse efectuado en sistemas que estén desarrollándose, por lo que no puede garantizarse que dichas mediciones sean iguales en los sistemas de los que se dispone habitualmente. Además, algunas de las mediciones pueden haberse estimado mediante extrapolaciones. Los resultados reales podrían ser distintos. Los usuarios de este documento deberían comprobar cuáles son los datos que se aplican a su entorno específico.

La información referente a productos que no son de IBM procede de los proveedores de dichos productos, sus anuncios publicados y demás información disponible para el público. IBM no ha probado dichos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni atender cualquier otra reclamación relacionada con productos que no sean de IBM. Las preguntas relacionadas con las posibilidades de productos que no sean de IBM deben dirigirse a los proveedores de dichos productos.

Cualquier manifestación de IBM sobre futuros planteamientos o propósitos podrá modificarse o anularse sin necesidad de aviso previo y representa únicamente finalidades y objetivos.

Los precios de productos IBM indicados en esta publicación son sugerencias de precios al por menor, son actuales y pueden modificarse sin previo aviso. Los precios de los concesionarios pueden variar.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales habituales. Para ilustrarlos lo mejor posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y direcciones de empresas comerciales reales es pura coincidencia.

Marcas registradas

Los siguientes términos son marcas registradas de International Business Machines en los Estados Unidos de América y/u otros países:

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

Otros nombres de empresas, productos y servicios pueden ser marcas comerciales o marcas de servicio de otras compañías.

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape y logotipos de Netscape	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y/u otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/u otros países.

UNIX es una marca registrada en los Estados Unidos y/u otros países cuyas licencias concede exclusivamente X/Open Company Limited.

Índice

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Hoja de Comentarios

IBM® SecureWay® Policy Director
Funcionamiento y ejecución
Versión 3 Release 0

Número de Publicación SCT6-3KES-00

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	□	□	□	□	□

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep-table	Insatisfecho	Muy insatisfecho
Organización	□	□	□	□	□
Información completa y precisa	□	□	□	□	□
Información fácil de encontrar	□	□	□	□	□
Utilidad de las ilustraciones	□	□	□	□	□
Claridad de la redacción	□	□	□	□	□
Calidad de la edición	□	□	□	□	□
Adaptación a los formatos, unidades, etc. del país	□	□	□	□	□

Comentarios y sugerencias:

Nombre

Dirección

Compañía u Organización

Teléfono

Hoja de Comentarios
SCT6-3KES-00

Corte o Doble
Por la Línea

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

SCT6-3KES-00

Corte o Doble
Por la Línea

Número Pieza: CT63KES

Printed in Ireland

CT63KES

SCT6-3KES-00