IBM SecureWay Policy Director
Versión 3.0
Guía de administración

IBM SecureWay Policy Director
Versión 3.0
Guía de administración

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información general que aparece en el "Apéndice B. Avisos" en la página 301.

Primera edición (octubre de 1999)

Este manual es la traducción del original inglés Policy Director Administration Guide. Esta edición se refiere a la versión 3, release 0, nivel de modificación 0 del producto IBM® FirstSecure SecureWay® Policy Director™ y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Esta edición sustituye la versión 2, release 2, nivel de modificación 2.00 de IBM SecureWay Global Sign-On™.

Contenido

Acerca de este manual

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**).

Destinatarios de este manual

Este manual se dirige a los administradores que vayan a gestionar usuarios, grupos, recursos GSO, grupos de recursos GSO, usuarios proxy, listas de control de accesos, permisos y el espacio de objetos de Policy Director.

La persona que administre Policy Director también deberá gestionar los servicios de autentificación, de autorización y la adquisición de credenciales y habrá de tener algunos conocimientos sobre estos procesos.

El administrador también debe tener conocimientos sobre la gestión 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 Servers que están incluidos en el producto Policy Director.

Organización de este manual

Este manual se ha organizado en las siguientes secciones:

- Los capítulos 1 a 3 describen conceptos sobre Policy Director como, por ejemplo, la visión general de Policy Director que se encuentra en el “Capítulo 1. Bienvenidos a Policy Director” en la página 1, el “Capítulo 2. Autentificación y adquisición de credenciales” en la página 17 y el “Capítulo 3. Qué es una autorización” en la página 37.
- Los capítulos 4 a 12 explican tareas generales de administración de Policy Directory como, por ejemplo:
  - “Capítulo 4. Presentación de Management Console” en la página 57
  - “Capítulo 5. Gestión de cuentas de usuarios y de grupos” en la página 71
  - “Capítulo 6. Gestión de recursos GSO, grupos de recursos y credenciales de recursos” en la página 77
  - “Capítulo 7. Qué es el control de acceso” en la página 83
  - “Capítulo 8. Aplicación del control de acceso” en la página 109
  - “Capítulo 9. Gestión de usuarios proxy” en la página 115
  - “Capítulo 10. Gestión de servidores de Policy Director” en la página 125
  - “Capítulo 11. Gestión del servicio de autorizaciones” en la página 135
  - “Capítulo 12. Registro cronológico y auditoría de la actividad del servidor” en la página 147

Los capítulos 13 a 16 tratan de la administración de WebSEAL:

- “Capítulo 13. WebSEAL: Configuración de la autentificación” en la página 161
- “Capítulo 14. WebSEAL: Tareas generales de administración” en la página 181
- “Capítulo 15. WebSEAL: administración de Smart Junction” en la página 191
- “Capítulo 16. WebSEAL: integración de aplicaciones” en la página 221

Los capítulos 17 y 18 analizan los siguientes temas de administración de NetSEAL:
- “Capítulo 17. NetSEAL: visión general” en la página 231
- “Capítulo 18. NetSEAL: Tareas generales de administración” en la página 245

Los capítulos 19 a 21 proporcionan información sobre la administración de NetSEAT:
- “Capítulo 19. NetSEAT: Visión general” en la página 253
- “Capítulo 20. NetSEAT: Tareas generales de administración” en la página 259
- “Capítulo 21. NetSEAT: Directory Services Broker” en la página 275

En el manual se incluyen los siguientes apéndices: “Apéndice A. Administración de Policy Director utilizando ivadmin” en la página 279 y “Apéndice B. Avisos” en la página 301.

Convenios utilizados en este manual

Este manual utiliza los siguientes convenios tipográficos:

Convenio	Significado
negrita	Elementos de la interfaz de usuario como, por ejemplo, nombres de menús, elecciones de menús, campos de entrada, iconos, carpetas, cuadros de listas, botones de acción, pulsadores, botones de selección, selectores cíclicos y recuadros de selección. Para las notas y avisos se utiliza también la negrita.
`monospace`	Sintaxis, código de ejemplo y 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: Seleccione **Archivo → Ejecutar** significa Pulse el botón en **Archivo** y después pulse el botón en **Ejecutar**.

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 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.

Requisitos previos e información pertinente

Consulte la siguiente documentación si necesita más información sobre los requisitos previos de Policy Director y los productos relacionados con él.

IBM SecureWay Policy Director

Documentación en formato PDF: Las siguientes publicaciones están relacionadas con Policy Director y pueden encontrarse en formato PDF bajo /doc en el CD de *IBM SecureWay Policy Director Versión 3.0*:

- Este manual, *IBM SecureWay Policy Director Guía de Administración, Versión 3.0*
- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

Documentación en formato impreso: El siguiente manual también está relacionado con Policy Director y está disponible en formato impreso con el paquete del producto:

IBM SecureWay Policy Director Up and Running, Version 3.0 (SCT6-3KNA-00)

IBM SecureWay FirstSecure

El siguiente documento está relacionado con IBM SecureWay FirstSecure:

- *IBM SecureWay FirstSecure Planning and Integration, Version 2.0 (S564-8D11-00)*

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

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.

IBM DCE para Windows NT

IBM Distributed Computing Environment for Windows NT Quick Beginnings, Version 2.2, 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.

IBM DCE para AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2, está disponible en la siguiente dirección 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.

Transarc DCE para Solaris

Las publicaciones *Transarc DCE Version 2.0 Release Notes* e *Installation and Configuration Guide* están disponibles en la siguiente dirección 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
- Defectos y limitaciones conocidos asociados a DCE DFS

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

IBM SecureWay Directory

Se dispone también de los siguientes documentos para IBM SecureWay Directory:

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

  Existe una versión distinta de este manual para cada sistema operativo soportado.
- *IBM SecureWay Directory Client SDK Programming Reference*
- *IBM SecureWay Directory Server Plug-ins Reference*

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 que corresponde a cada sistema operativo se encuentra en el CD pertinente. Los CD son los siguientes:
  - *IBM SecureWay Directory Versión 3.11 para NT*
  - *IBM SecureWay Directory Versión 3.11 para AIX*
  - *IBM SecureWay Directory Versión 3.11 para Solaris*

Se dispone también de los siguientes documentos para IBM SecureWay Directory:

- *IBM SecureWay Directory Client SDK Programming Reference*
- *IBM SecureWay Directory Server Plug-ins Reference*

Cómo enviar comentarios

Su experiencia es importante para ayudarnos a proporcionar una información precisa y de alta calidad. Si tiene algún comentario sobre este manual o cualquier otra documentación de IBM SecureWay Policy Director, visite la página de presentación de Policy Director en:

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

Encontrará allí la página de ″feedback″ donde podrá entrar sus comentarios y enviarlos. También encontrará información sobre las actualizaciones más recientes de Policy Director.

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

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

Capítulo 1. Bienvenidos a Policy Director

IBM SecureWay Policy Director (Policy Director) es una completa solución de autorizaciones para aplicaciones empresariales de la Web, de cliente/servidor y heredadas. El sistema de autorizaciones de Policy Director permite a una organización controlar de forma segura el acceso de usuarios a información protegida. Policy Director se utiliza junto con aplicaciones estándar basadas en Internet para crear intranets bien gestionadas y altamente seguras.

Este capítulo incluye los siguientes temas:

Qué es la seguridad de redes de empresas

Muchas organizaciones valoran ahora la Internet pública y las intranets privadas como medios efectivos y vitales para la comunicación global. El comercio electrónico se está convirtiendo ahora en un componente esencial de muchas de las estrategias comerciales empresariales. Las instituciones docentes confían en Internet para el estudio a distancia. Los servicios en línea permiten a los usuarios enviar correo electrónico y utilizar los enormes recursos enciclopédicos de la Web. Las aplicaciones tradicionales, como TELNET o POP3, siguen predominando como importantes servicios de red.

Las empresas se dan cuenta de que pueden utilizar las tecnologías de Internet para mejorar sus relaciones con las cadenas de abastecimientos, facilitar la colaboración entre sus socios comerciales y proporcionar a los clientes una mejor conectividad. Las empresas pueden disponer de todo esto siempre y cuando puedan exponer sus recursos empresariales con un alto grado de seguridad.

Las empresas desean utilizar Internet como vehículo global comercial y de distribución. Sin embargo, la falta de sistemas de gestión y mecanismos con una política de seguridad probada obstaculiza este tipo de negocios.

Policy Director es una solución de gestión de políticas de información que proporciona a las empresas servicios centralizados de seguridad de redes. Con estos servicios centralizados de seguridad de redes, se puede tener y mantener información coherente sobre usuarios y políticas.

Terminología y definiciones de seguridad de redes

Los siguientes servicios y conceptos de seguridad son importantes para el análisis de Policy Director a lo largo de este documento:

Dominio seguro
: El grupo de usuarios, sistemas y recursos que comparten servicios comunes y, normalmente, funcionan con una finalidad común.

Autentificación
: El proceso en el que se identifica a un individuo que intenta iniciar una sesión en un dominio seguro.

Credenciales Información detallada adquirida durante la autentificación que

describe al usuario, las asociaciones de grupos (si las hay) y demás atributos de identidad relacionados con la seguridad.

Autorización Proceso en el que se determina si un individuo tiene derechos para realizar una operación en un recurso protegido.

Cifrado Conversión de datos electrónicos en código secreto que protege dichos datos para que no puedan ser examinados por entes o personas no autorizados.

Integridad Condición en la que los datos electrónicos no cambian desde que se envían hasta que se reciben.

Calidad de protección
Nivel de seguridad de los datos que se determina mediante la combinación de las condiciones de autentificación, integridad y privacidad.

Escalabilidad Posibilidad de un sistema de red de aumentar el número de usuarios que acceden a recursos.

Factores comunes de la seguridad de redes

Tanto la red pública mundial Internet como las intranets privadas de las empresas se conectan a redes, aplicaciones y sistemas informáticos heterogéneos. Esta mezcla de distintos hardware y software afecta normalmente a la red de estas formas:

- No hay un control de seguridad centralizado para las aplicaciones.
- No hay un convenio unificado de denominación de la ubicación de recursos.
- No hay un soporte común para una alta disponibilidad de las aplicaciones.
- No hay un soporte común para un crecimiento escalable.

Los nuevos modelos comerciales requieren que las empresas expongan sus recursos de información de una forma que nunca antes se hubiese imaginado. Estas empresas deben saber que pueden controlar con seguridad el acceso a dichos recursos.

Se ha demostrado que la gestión de políticas y usuarios a través de redes distribuidas resulta muy difícil para los gestores de tecnología de la información (Information Technology, IT). Y resulta difícil porque proveedores individuales de aplicaciones y sistemas conceden las autorizaciones cada uno a su manera.

Las compañías comprenden que desarrollar nuevos servicios de autorización para cada aplicación de la empresa es un proceso caro que conduce a infraestructuras difíciles de gestionar. Un servicio de autorizaciones centralizado al que puedan acceder los programadores utilizando una interfaz de programas de aplicación (API) podría acelerar enormemente el tiempo de las compras y reducir el coste total de explotación.

Un sistema de gestión de seguridad de la red centralizado debe cumplir con una serie de requisitos como, por ejemplo:

- Coexistencia con las arquitecturas existentes de cortafuego y autentificador y potenciación de las mismas.
- Integración o coexistencia con infraestructuras de gestión de redes y aplicaciones.
- Independencia de las aplicaciones.

Presentación de Policy Director

Policy Director es una completa solución de autorizaciones, seguridad de redes y gestión de políticas que proporciona una inmejorable 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 accesos y de seguridad para restringir a determinados abonados la utilización de una o más intranets conectadas a Internet.

Además de su modernísima función de gestión de políticas de seguridad, Policy Director tiene soporte para funciones de autentificación, autorizaciones, seguridad de datos y gestión de recursos. Policy Director se utiliza junto con aplicaciones estándar basadas en Internet para crear intranets bien gestionadas y altamente seguras.

Con Policy Director, las empresas pueden gestionar ahora el acceso a recursos internos privados basados en redes. Las empresas también pueden potenciar la amplia conectividad y la fácil utilización de la Internet pública. Policy Director, combinado con un sistema cortafuego de la empresa, puede proteger a la intranet de una compañía contra accesos e intrusiones no autorizados.

Estándar de la API de Policy Director Authorization Service

Los *servicios de autorizaciones* son una parte crítica de la arquitectura de seguridad de una aplicación. Cuando un usuario ha pasado el proceso de autentificación, los servicios de autorizaciones proceden a ejecutar la política de la empresa determinando a qué servicios e información puede acceder el usuario.

Por ejemplo, un usuario que acceda a un fondo de pensiones a través de la Web podrá ver información personal de su cuenta. Para que esto pueda llevarse a cabo, un servidor de autorizaciones deberá verificar los atributos de identidad, credenciales y privilegios de dicho usuario.

La API de autorizaciones de Policy Director basada en estándares permite a las aplicaciones efectuar llamadas al Policy Director Authorization Service centralizado. Al realizar estas llamadas se elimina la necesidad de que los programadores escriban código de autorización para cada nueva aplicación.

La API de autorizaciones de Policy Director permite a las empresas estandarizar todas las aplicaciones sobre una infraestructura de autorizaciones fiable. Con la API de autorizaciones de Policy Director, las empresas pueden proporcionar más control para el acceso a recursos de sus redes.

En el manual *Policy Director Programmer's Guide and Reference* puede ver las descripciones de la API de autorizaciones de Policy Director.

Tecnologías esenciales de Policy Director

La solución de gestión de seguridad de redes de Policy Director proporciona y soporta las siguientes tecnologías básicas:

- Autentificación
- Autorización
- Calidad de protección de datos
- Escalabilidad
- Contabilidad

Autentificación

Esta tecnología básica incluye soporte para los *mecanismos de autentificación* de nombre de usuario y contraseña de Policy Director.

Clave secreta:

- Kerberos
- Lightweight Directory Access Protocol (LDAP)

Clave pública/privada:

- Inicie la sesión a través de un navegador habilitado para Secure Socket Layer (SSL), utilizando un nombre de usuario y una contraseña específicos de las aplicaciones:
  - Mecanismo de autentificación básica (BA)—sólo WebSEAL y la interfaz de Secure Socket Layer HTTPS.
  - Mecanismo basado en formularios de Policy Director—sólo WebSEAL y HTTPS
- Inicie la sesión a través de SSL utilizando el certificado X.509 del área del cliente—Policy Director tiene soporte para productos de infraestructura de clave pública (PKI) que cumplen con las normas PKIX (como IBM SecureWay Trust Authority, Versión 3.1) o productos PKI basados en Entrust (como IBM Vault Registry, Versión 2.2.2).

  IBM SecureWay Trust Authority Versión 3.1 incluye software de cliente, una simple aplicación de registro, una autoridad de certificación y un directorio integrado para dar soporte a todo el ciclo vital de un certificado que incluye la inscripción y la certificación inicial, la actualización del par de claves, la actualización del certificado, la publicación del certificado y de la lista de revocación de certificado (CRL) y la revocación del certificado. Se proporciona una interfaz gráfica de usuario (GUI) para gestionar las peticiones de autoridad de certificación (CA), autoridad de registro (RA) y entidad final (EE). También se facilita una biblioteca de API.

Adquisición de credenciales:

- Servicio de adquisición de credenciales (CAS)—extensiones de autentificación personalizadas.

Autorización

Esta tecnología básica proporciona soporte para los siguientes tipos en las autorizaciones de Policy Director;

- Policy Director Authorization Service
- La API de Policy Director Authorization basada en estándares
- Una posibilidad de autorización externa

Calidad de protección de datos

La *calidad de protección* indica el grado con el que Policy Director protege la información transmitida entre un cliente y un servidor. El efecto combinado de mecanismos de túnel (″tunnel″), estándares de cifrado y algoritmos de detección de modificaciones determina la calidad de protección.

Para aumentar la seguridad, los niveles de protección de datos incluyen:

1. Comunicación estándar con Transmission Control Protocol (TCP) (sin autentificación)
2. Sólo autentificación—verifica la identidad del usuario

3. Autentificación + integridad de datos—protege los mensajes (corriente de datos) para impedir su modificación durante la comunicación de la red
4. Autentificación + integridad de los datos + privacidad de los datos—protege los mensajes para que no puedan ser modificados ni examinados durante la comunicación por la red.

Puede indicar los niveles de protección que desea utilizar para redes y sistemas principales específicos.

Estándares de cifrado soportados: Policy Director tiene soporte para el siguiente estándar de cifrado de datos (Data Encryption Standard, DES) y otras codificaciones de cifrado a través de SSL:

- RC2 de 40 bits
- RC2 de 128 bits
- RC4 de 40 bits
- RC4 de 128 bits
- DES de 40 bits
- DES de 56 bits
- DES triple de 168 bits

Policy Director NetSEAL y Policy Director WebSEAL tienen soporte para cifrado DES de 40 bits y DES de 56 bits a través de DCE-Remote Procedure Call (DCE-RPC).

Nota: Las versiones internacionales pueden estar sujetas a las limitaciones de exportación de la tecnología de cifrado.

Mecanismos de tunelización: 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 módems. 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 el cliente NetSEAT presta servicio como cliente SSL a 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.

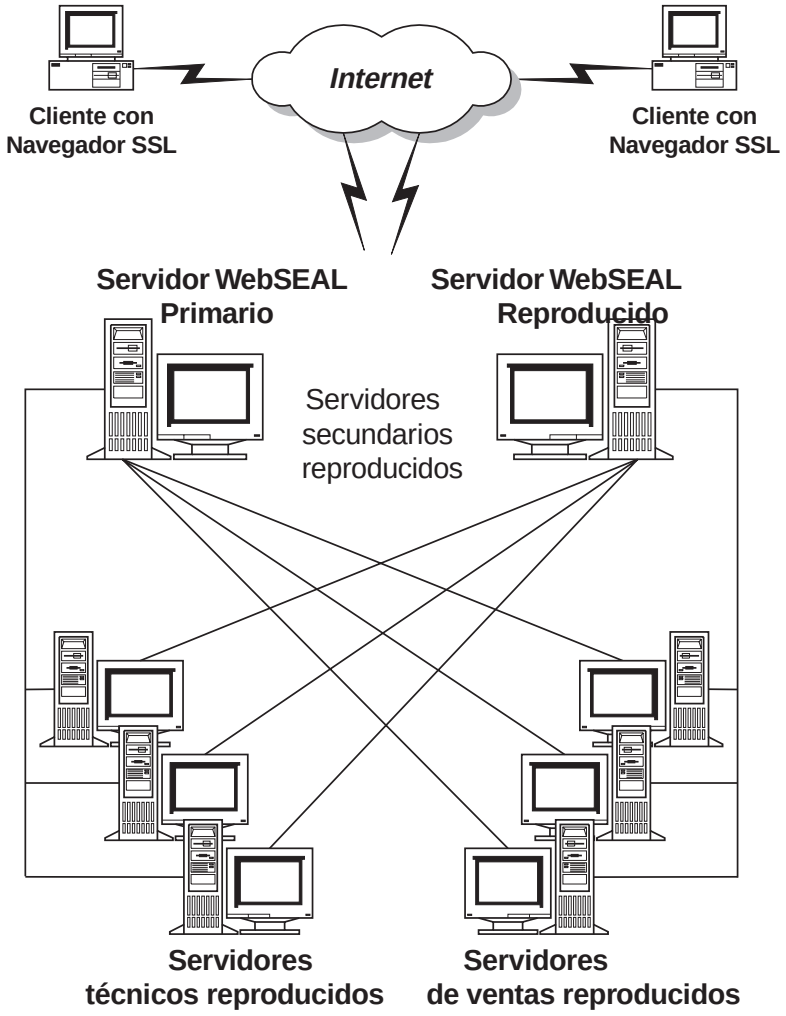
Tunelización (″tunnel″) de GSS: La interfaz Generic Security Service, GSS) es una forma estándar que permitir a las aplicaciones acceder a los servicios de seguridad. La tunelización (″tunnel″) de GSS se utiliza a través de RPC seguras. Habilite esta opción cuando instale un cliente NetSEAT como módulo 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, a nivel de fuente, la portabilidad de aplicaciones a distintos entornos. La tunelización habilita control sobre el nivel de protección del 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.

Escalabilidad

La *escalabilidad* es la posibilidad de responder al aumento del número de usuarios que acceden a recursos del dominio seguro. Policy Director utiliza las siguientes técnicas para proporcionar escalabilidad:

- Reproducción de servicios
  - Autentificación de servicios
  - Autorización de servicios
  - Políticas de seguridad
  - Servicios de cifrado de datos
  - Servicios de auditoría
- Reproducción de WebSEAL Servers secundarios
  - Reflexión de recursos para que haya una alta disponibilidad
  - Equilibrio de carga de peticiones de clientes
- Reproducción de servidores principales
  - Servidores principales, que pueden ser servidores WebSEAL o servidores Web de terceros
  - Recursos reflejados (espacio de nombres unificado) para tener una alta disponibilidad
  - Contenidos y recursos adicionales
  - Equilibrio de la carga de peticiones entrantes a través de tecnología Smart Junction™
- Rendimiento óptimo al permitir la descarga de los servicios de autentificación y autorización para distintos servidores
- Despliegue escalado de los servicios sin aumentar la actividad general de gestión



Contabilidad

Policy Director tiene varias posibilidades de registro cronológico y auditoría. Tiene archivos de anotaciones cronológicas que captan todos los mensajes de error y todos los mensajes de aviso generados tanto por servidores Policy Director Server como DCE Server. También tiene archivos de seguimiento de auditoría que supervisan la actividad de los servidores de Policy Director y DCE.

Archivos de anotaciones cronológicas

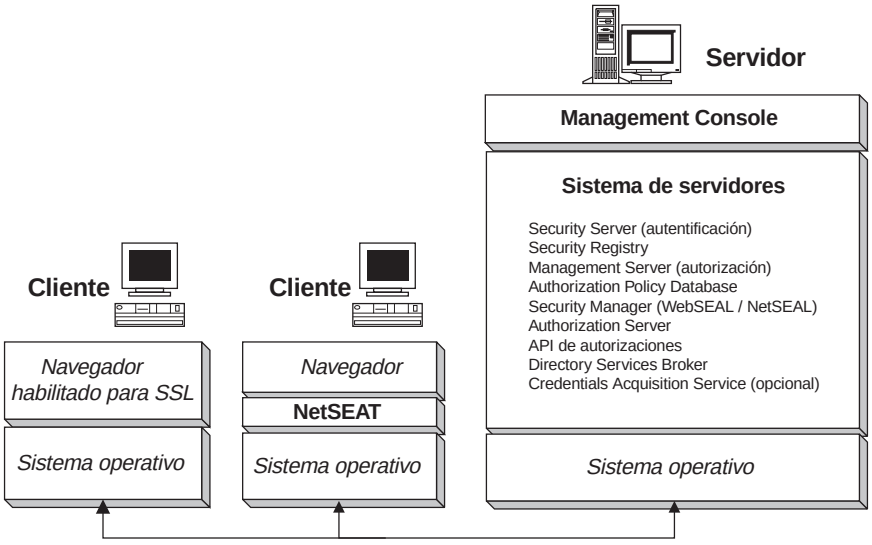
- Archivos de anotaciones cronológicas de Policy Director Server
- Archivos de anotaciones cronológicas de DCE Server
- Mensajes de servicios DCE
- Archivos de anotaciones cronológicas de HyperText Transfer Protocol (HTTP) estándar.

Archivos de seguimiento de auditoría

- Archivos de seguimiento de auditoría de autorizaciones de Policy Director
- Archivo de seguimiento de auditoría de WebSEAL
- Archivo de seguimiento de auditoría de gestión de Policy Director
- Archivo de seguimiento de auditoría de DCE
- Archivo de seguimiento de auditoría de LDAP

Componentes de Policy Director

Policy Director incluye software para sistemas cliente y sistemas servidor. Policy Director proporciona soporte para los sistemas operativos Solaris, IBM AIX y Microsoft® Windows NT®.



Management Console

Management Console es una aplicación gráfica basada en Java® que se utiliza para gestionar la política de seguridad del dominio seguro de Policy Director. Desde Management Console, se pueden realizar tareas administrativas en el registro de contabilidad y en la base de datos primaria de políticas de autorización (también llamada *maestra*).

Entre las tareas habituales de Management Console se encuentran la inclusión y supresión de cuentas de usuarios y de cuentas de grupos, así como la aplicación de listas de control de accesos (ACL) a objetos del espacio de nombres. Management Console utiliza RPC para realizar estas tareas de gestión a través de canales de comunicación seguros.

Las responsabilidades de gestión pueden delegarse al nivel local. Por ejemplo, puede asignar un administrador de seguridad con responsabilidades limitadas. Dicho administrador de seguridad podrá gestionar entonces la política de seguridad únicamente para los recursos localizados en la porción designada del espacio de nombres de objetos protegidos.

Security Server

El Security Server (secd) puede ser un servidor LDAP o un servidor DCE. Este servidor proporciona servicios de autentificación. También mantiene una base de datos centralizada (LDAP o DCE) de registros que contiene las entradas de las cuentas de todos los usuarios válidos que participan del dominio seguro.

En un entorno DCE, los usuarios de la base de datos de registros se denominan a veces *principales*.

El Security Server tiene dos funciones importantes:

- El Security Server define los grupos y organizaciones a los que pertenece el usuario y las funciones que dicho usuario puede ejecutar. La base de datos de

registros almacena esta información. Policy Director Authorization Service tiene en cuenta esta información cuando toma decisiones sobre autorizaciones.

- El Security Server proporciona servicios de autentificación para todos los intentos de inicio de sesión.

Para DCE, Security Server puede reproducir la base de datos de registros en todo el dominio seguro para impedir que haya un solo punto de error. El Security Server es el responsable de la actualización de todas las réplicas de bases de datos siempre que se produce un cambio en el registro primario.

Management Server

Management Server (ivmgrd) mantiene la base de datos primaria de políticas de autorización para el dominio seguro. También es el responsable de la actualización de todas las réplicas de la base de datos de autorización en todo el dominio seguro. Management Server mantiene así mismo la información de ubicación de los demás servidores de Policy Director en el dominio seguro.

Security Manager

El Security Manager (secmgrd) aplica una política de control de accesos basada en información procedente de una réplica de una base de datos de políticas de autorización. Security Manager incluye:

- Un componente NetSEAL para un control de accesos flexible de Transmission Control Protocol/Internet Protocol (TCP/IP).
- Un componente WebSEAL para un control de accesos rígido de HTTP y HTTPS.

WebSEAL

WebSEAL es uno de los dos componentes de Security Manager (secmgrd).

WebSEAL es un servidor Web de múltiples hebras y de alto rendimiento que acepta peticiones de clientes HTTP, HTTPS y NetSEAT. WebSEAL gestiona el control de accesos para recursos como, por ejemplo:

- Universal Resource Locations (URL)
- expresión regular basada en URL
- Programas Common Gateway Interface (CGI) en Perl, C™, o C++
- archivos Hypertext Markup Language (HTML)
- servlets Java
- archivo de clase Java

WebSEAL, como servidor de conexiones (junction) asegura y gestiona servidores de la Web de terceros mediante la tecnología Smart Junction. Las *conexiones Smart Junction* permiten conectar al espacio de la Web sistemas de archivos de servidor adicionales y ver los recursos como si se tratase de un solo espacio de nombres de objetos unificado.

Utilice WebSEAL para facilitar posibilidades de inicio de sesión único de recursos basados en la Web. El usuario se autentifica ante WebSEAL utilizando Kerberos o SSL estándar. A continuación, WebSEAL identifica al usuario utilizando la autentificación básica y la autentificación resumida de HTTP. WebSEAL también puede pasar la identidad del usuario como variable CGI.

NetSEAL

NetSEAL es uno de los dos componentes de Security Manager (secmgrd). NetSEAL es una solución de Virtual Private Network (VPN) para asegurar todas las

comunicaciones entrantes de TCP/IP. NetSEAL realiza el control de accesos basándose en la puerta de destino y en la identidad del cliente. NetSEAL es la solución de seguridad para

- Autorizar y asegurar servicios de Internet tradicionales, como TELNET y POP3.
- Autorizar y asegurar varios paquetes de aplicaciones como, por ejemplo sistemas de bases de datos y herramientas de gestión.

NetSEAL es un gestor de recursos que controla la posibilidad de un usuario de conectarse a una puerta determinada del servidor (por ejemplo, la puerta 23, TELNET). El componente NetSEAL también acepta y autoriza el tráfico TCP/IP tunelizado a partir del cliente NetSEAT.

La utilización del servidor NetSEAL permite la integración de cualquier servidor de aplicaciones de la red con servicios de seguridad de Policy Director. El NetSEAL Server proporciona un punto de terminación de túnel (″tunnel″) seguro para todas las comunicaciones de la red. La identidad autentificada del usuario se pasa junto con la petición de protocolo original a través de este túnel creado por SSL o GSS. Utilice túneles NetSEAL SSL para comunicarse con el cliente NetSEAT.

Cliente NetSEAT

NetSEAT es un módulo de soporte de red. Este módulo funciona sin problemas como proxy seguro para aplicaciones de cliente al permitir un cifrado de principio a fin, por un túnel SSL o GSS, del tráfico de todos los clientes/servidores. Como implementación de Dynamic Link Library (DLL) de un cliente de seguridad, NetSEAT permite a los usuarios aprovechar al máximo las características de Policy Director. Entre estas características se encuentran el asegurar las comunicaciones de datos y el proporcionar una arquitectura de alta disponibilidad.

NetSEAT asegura una integración completa con el mecanismo de seguridad de Policy Director y permite la gestión de recursos para el cliente. NetSEAT proporciona protección a las aplicaciones TCP/IP. NetSEAT cifra los datos de la aplicación de forma trasparente en túneles (″tunnels″) VPN (como los SSL o GSS) que pueden transportarse a través de enlaces inseguros (como la Internet púbica)).

Puede configurarse para interceptar todas las peticiones HTTP y para enviarlas al WebSEAL Server de destino. Correlaciona de forma transparente URL lógicos con WebSEAL Server físicos al permitir la reubicación o reproducción de recursos de la Web, sin que ello afecte al usuario final.

Nota: NetSEAT no es necesario para interactuar con Policy Director. Por ejemplo, los usuarios cliente pueden utilizar navegadores habilitados para SSL para comunicarse directamente con WebSEAL.

API de autorizaciones

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 las 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.

La API de autorizaciones de Policy Director reduce el tiempo de desarrollo de aplicaciones así como el coste de dicho desarrollo. Como la API de autorizaciones

proporciona una gestión centralizada de toda la seguridad de la red, el coste total de la explotación y la probabilidad de violaciones de la seguridad de la red se reducen significativamente.

Authorization Server

En modalidad de autorización de antememoria remota, las aplicaciones utilizan las llamadas de función proporcionadas por la API de autorizaciones de Policy Director para comunicarse con el Authorization Server de Policy Director (ivacld). El Authorization Server de Policy Director mantiene una réplica de la base de datos de políticas de autorización y funciona como evaluador de toma de decisiones de autorización.

La API de Policy Director Authorization envía una petición de decisión de autorización a Policy Director Authorization Server. Policy Director Authorization Server devuelve una recomendación basada en la política de seguridad. El servidor también puede grabar un registro de auditoría que contenga los detalles de la petición de autorización.

Directory Services Broker

Policy Director instala y configura automáticamente Directory Services Broker (DSB) durante la instalación de Policy Director. Policy Director proporciona el producto DSB como parte del paquete de Management Server (IVMgr). No es necesario efectuar ninguna otra operación para utilizar un DSB.

Si los clientes NetSEAT sirven como módulo de soporte de los Policy Director Server y de Management Console, utilizarán el DSB. Si los clientes NetSEAT utilizan únicamente la tunelización de SSL, no utilizarán el DSB.

El DSB actúa como servidor Cell Directory Services (CDS) de la gama media. El cliente NetSEAT dirige al DSB las peticiones de ubicación de recursos y servicios. El DSB, a su vez, se pone en contacto con CDS para resolver la petición. A continuación, el DSB devuelve la información solicitada al sistema que ejecuta el cliente NetSEAT.

Credentials Acquisition Service (opcional)

Policy Director Credentials Acquisition Service (CAS) es un componente opcional. Policy Director instala automáticamente Credentials Acquisition Service durante la instalación de Policy Director.

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 las credenciales.

Los clientes SSL procedentes de un registro externo que no sean de Policy Director, pueden correlacionar sus *nombres de usuarios* con identidades de Policy Director a través de Policy Director Credentials Acquisition Service o escribiendo un servicio propio de adquisición de 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.

También 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 y 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 a 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.

Qué es el modelo de seguridad

En Policy Director, seguridad significa acceso controlado a la información. La tecnología de Policy Director correlaciona la política de seguridad de una organización con los objetos del espacio de nombres protegidos.

Este acceso puede basarse en políticas empresariales sin las limitaciones que implica la topología de la red. Se puede permitir o denegar el acceso de usuarios basándose en quiénes son y en la función que realizan en vez de en su ubicación física.

Los componentes de Policy Director son aplicaciones basadas en servidores y clientes. La utilización de la autentificación mutua y de la asignación de derechos de acceso le permitirá lograr una disponibilidad general de algunos recursos. Y, al mismo tiempo, podrá restringir los recursos internos más confidenciales para que su acceso sea autorizado y más seguro. Su información estará segura independientemente de si un usuario autorizado accede a los datos desde dentro del dominio seguro o utilizando una conexión remota a Internet.

Definición de una política de seguridad

El software de seguridad de Policy Director permite crear un dominio seguro en el que todas las comunicaciones están protegidas contra accesos no autorizados y corrupciones no detectadas.

El administrador de un dominio seguro debe averiguar:

- Quién puede participar del dominio seguro y puede solicitar el acceso a objetos en el espacio de nombres de objetos protegidos.
- Qué objetos deben protegerse.
- Qué normas protegen a estos objetos.

Policy Director procesa una petición de cliente de la siguiente forma:

- Demuestra quién es el cliente utilizando la autentificación.
- Adquiere derechos en forma de credenciales de autorización.
- Toma una decisión de autorización basándose en dichas credenciales.

¿Quién puede participar del dominio seguro?

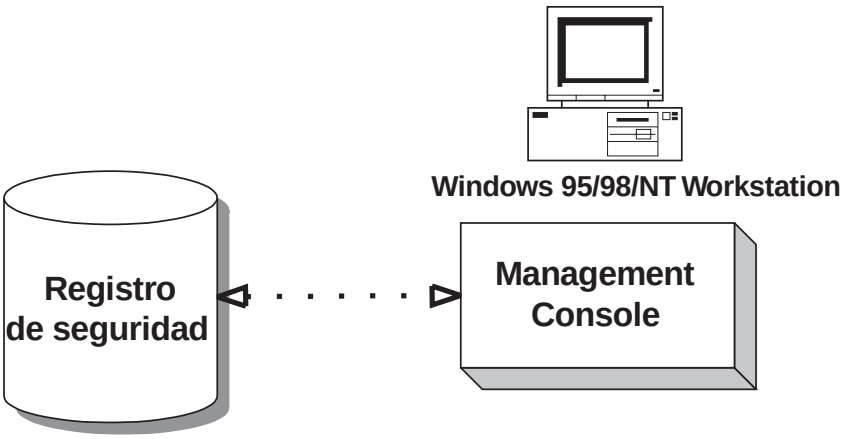
El administrador mantiene una lista oficial de los usuarios (llamados *principales* en el entorno DCE) y grupos que sean miembros del dominio seguro de Policy

Director. Esos usuarios y grupos podrán, por lo tanto, participar en el acceso a recursos. La base de datos de registros (LDAP o DCE) almacena esa información de usuarios y grupos.

Podrá autorizar a un usuario a participar en el dominio seguro tan pronto como haya creado una cuenta para él.

Tarea administrativa:

- Crear cuentas de usuarios y grupos utilizando Management Console (o el mandato **ivadmin**.



¿Qué objetos deben protegerse y mediante qué normas?

Policy Director puede proteger los siguientes tipos de recursos:

- Objetos de la Web, como archivos HTML, programas CGI y HTML dinámico
- Servicios de la red asegurados por NetSEAL (como, por ejemplo, TELNET, POP3 y aplicaciones personalizadas)
- Funciones de gestión

Policy Director representa recursos reales como objetos en un espacio de nombres de objetos protegidos. Los permisos de acceso específicos se asignan uniendo *plantillas de políticas* a dichos objetos. Policy Director utiliza un tipo de plantilla de política conocido como *lista de control de accesos* (access control list, ACL). Una ACL define:

- Quién puede acceder al objeto.
- Qué operaciones pueden llevarse a cabo en el objeto.

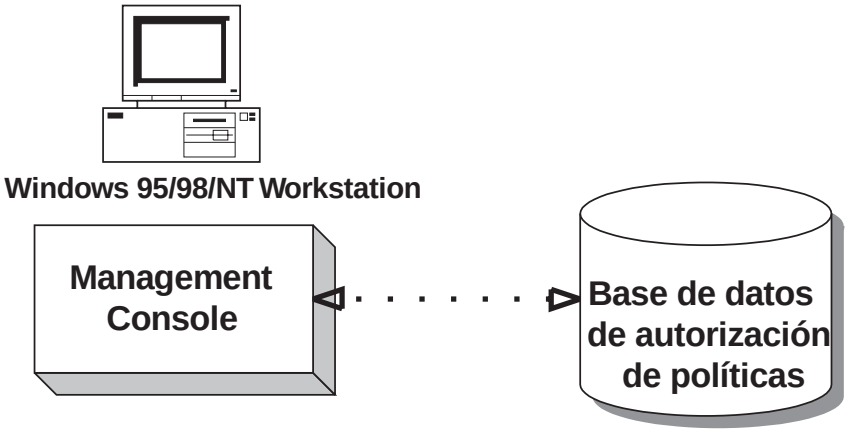
Por ejemplo, se pueden otorgar privilegios de visualización del objeto a todos los grupos y permitir a un solo grupo modificar el objeto.

Policy Director utiliza un mecanismo para definir permisos globales que se conoce como *modelo de ACL breve (o heredada).* En el modelo breve de ACL, la ACL no se aplica directamente a todos los objetos de la jerarquía. En su lugar, el modelo utiliza valores heredados de la ACL. Si un objeto de la jerarquía no tiene aplicada ninguna ACL, la ACL efectiva será la inmediatamente anterior de la jerarquía. Se requiere una ACL en el objeto root (/) para que todos los objetos puedan tener una ACL que heredar.

Utilizando el mecanismo de permisos globales no tendrá que definir permisos para cada archivo o directorio.

Tarea administrativa:

- Definir una política de seguridad para el espacio de nombres utilizando Management Console para aplicar plantillas de políticas (ACL) a objetos que requieran protección.

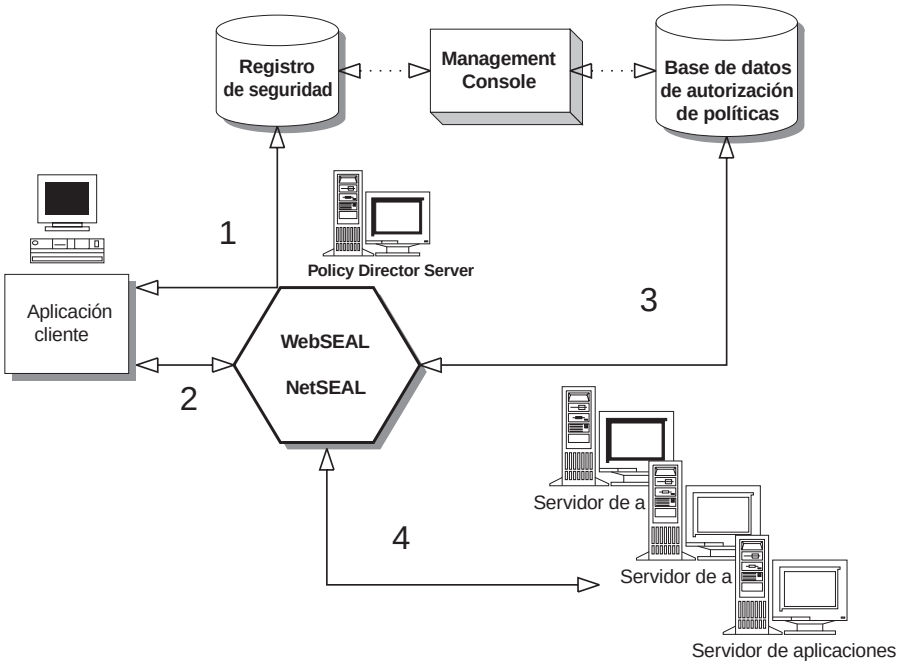


Aplicación de una política de seguridad a una petición de cliente

Cuando un usuario solicita el acceso a una aplicación u objeto protegido, Policy Director realiza las comprobaciones adecuadas de autentificación y autorización antes de aprobar la petición.

1. El usuario cliente se autentifica ante el Security Server para establecer una prueba de identidad. Policy Director soporta la autentificación mediante métodos de claves públicas y de claves secretas.

   Basándose en esa identidad, el Security Server devuelve las credenciales de autorización del usuario. Las credenciales definen los grupos y organizaciones a los que pertenece el usuario y las funciones que dicho usuario puede realizar.



2. Se establece un túnel de comunicación segura entre el usuario cliente y Policy Director Server.
3. Se lleva a cabo una comprobación de autorización en una réplica centralizada de una base de datos de políticas de autorización. Policy Director impone las ACL basadas en las credenciales del usuario.
4. Si los valores del permiso son los adecuados para las credenciales del usuario, Policy Director pasa la petición al servidor de aplicaciones para completar la transacción.

Capítulo 2. Autentificación y adquisición de credenciales

La autentificación es el proceso en el que se identifica a un individuo que intenta iniciar la sesión con un dominio seguro. Los objetivos de la autentificación son demostrar la identidad de un cliente y obtener las credenciales que lo describan. Policy Director puede utilizar credenciales para la autorización, la auditoría y demás servicios.

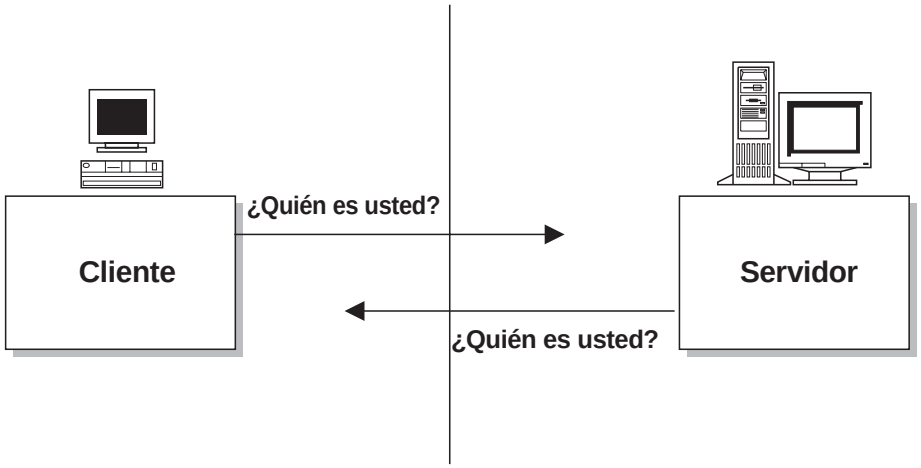
Este capítulo incluye los siguientes temas:

Conceptos básicos de la autentificación

Cuando los servidores ponen en vigor la seguridad en un dominio seguro, cada cliente debe proporcionar una prueba de su identidad. Cuando el acceso a cada recurso de un dominio seguro lo controla un servidor, las peticiones de autentificación y autorización del servidor pueden proporcionar una amplia seguridad en la red.

La *autentificación* es el proceso en el que se identifica a un individuo que intenta iniciar la sesión con un dominio seguro.

En los sistemas de seguridad, la autentificación es distinta de la autorización. La *autorización* determina si un usuario autentificado tiene derecho a realizar una operación en un recurso específico. La autentificación asegura que los individuos sean quienes dicen ser, pero no dice nada sobre la posibilidad de realizar operaciones en un recurso.



Policy Director tiene un planteamiento flexible de la autentificación que permite basar la política de seguridad en las necesidades de la empresa y no en la topología física de la red.

Policy Director autentifica la identidad de los usuarios cuando inician la sesión con un dominio seguro para acceder a información protegida. Los usuarios pueden asumir varias funciones, cada una de ellas con un permiso de acceso distinto.

Finalidades de la autentificación

El proceso de autentificación tiene dos finalidades importantes:

1. Determinar la identidad del cliente.
2. Adquirir credenciales para dicho cliente.

El *mecanismo de autentificación* y el *mecanismo de adquisición de credenciales* son realmente dos procesos distintos. Policy Director tiene soporte para varios mecanismos de autentificación (consulte el apartado “Mecanismos de autentificación soportados”).

Policy Director también proporciona servicios por omisión y personalizables para la adquisición de credenciales. Un *servicio de adquisición de credenciales* correlaciona información de identidad específica del mecanismo con una credencial de Policy Director. Las credenciales de Policy Director utilizan el formato Extended Privilege Attribute Certificate (EPAC).

Cualquier servicio de Policy Director que necesite información acerca de un cliente utiliza *credenciales*. Policy Director puede potenciar la utilización de credenciales para que ejecuten diversos servicios como, por ejemplo: autorización, auditoría y delegación.

Mecanismos de autentificación soportados

Policy Director tiene soporte para *mecanismos de autentificación* basados en claves secretas y públicas / privadas:

Clave secreta:

- Kerberos Versión 5
- Lightweight Directory Access Protocol (LDAP)

Clave pública/privada:

- Inicie la sesión a través de SSL utilizando el certificado X.509 del área del cliente—Policy Director tiene soporte para productos de infraestructura de clave pública (PKI) que cumplan con las normas PKIX (como IBM SecureWay Trust Authority, Versión 3.1) o productos PKI basados en Entrust (como IBM Vault Registry, Versión 2.2.2).

  Para obtener credenciales, se requiere la ayuda de un servicio de adquisición de credenciales.

Tipos de autentificación

Policy Director tiene soporte para los siguientes tipos de autentificación:

- Autentificación SSL—para autentificación de Internet e intranet
- Autentificación de nombre de usuario y contraseña—para autentificación basada en la identidad del usuario
- Autentificación Kerberos—para autentificación de la red

Autentificación SSL

El protocolo Secure Socket Layer (SSL) proporciona autentificación, seguridad y privacidad a través de Internet. SSL utiliza:

- Cifrado de par de claves pública/privada para autentificación.
- Clave secreta para cifrar datos a través de la conexión SSL.

Como autentificador, el protocolo SSL tiene soporte pata autentificación de sólo servidor y autentificación mutua.

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

Detalles del protocolo

El protocolo SSL, creado en la parte superior de TCP/IP, es independiente de la aplicación. El protocolo SSL permite a protocolos de aplicaciones (como HTTP, FTP y TELNET) instalarse de forma transparente en la parte superior. El protocolo de comunicaciones de la Web HTTP que funciona por un canal SSL cifrado se conoce como *HTTPS*.

El protocolo SSL puede negociar claves de cifrado y autentificar el servidor antes de que la aplicación de comunicaciones de alto nivel intercambie datos . El protocolo SSL mantiene la seguridad y la integridad del canal de transmisión utilizando el cifrado, la autentificación y códigos de autentificación de mensajes.

Fiabilidad de terceros y autoridad de certificación

La autentificación de SSL depende de la fiabilidad fundamental de un tercero que responde de la veracidad de una o de las dos partes autentificadoras. Este tercero fiable se conoce como *autoridad de certificación* (CA).

Una CA es la responsable de emitir *certificados digitales* (identidades electrónicas) que identifican a individuos, grupos o sistemas que utilizan la red y que son la prueba ante cualquiera de que la CA confía en el propietario.

Al firmar digitalmente esos certificados, la CA une la identidad del propietario del certificado a la clave pública que contiene el certificado. Cualquiera que considere fiable a la CA también debe considerar fiable al usuario.

Los usuarios de la red pueden obtener el certificado de clave pública de la CA y utilizarlo para verificar los certificados de otros usuarios. Con esa verificación, tendrán la seguridad de que las claves públicas de los certificados son las claves auténticas de los propietarios nombrados y sabrán que la CA (a la que reconocerán y a quien considerarán fiable gracias al certificado root) responde de ese enlace.

Cuando dos partes autentificadas intercambien certificados de claves públicas, podrán proceder a cifrar y firmar digitalmente los datos de la sesión. El cifrado y la firma digital eliminan la posibilidad de que otros puedan participar sin autorización en la sesión o dañar los datos.

Una CA puede ser una empresa que vende certificados a través de Internet o puede ser un departamento responsable de la emisión de certificados en la intranet de la empresa. Es usted quien debe decidir las CA que considera suficientemente fiables para que verifiquen las identidades de otras personas.

Uno de los conjuntos de productos de seguridad de IBM SecureWay FirstSecure (FirstSecure) es IBM SecureWay Trust Authority (Trust Authority) . Este producto le

permitirá emitir sus propios certificados para la intranet de la empresa. La información más actualizada sobre FirstSecure y sus componentes se encuentra en el sitio Web:

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

Certificados digitales X.509

La autentificación a través de SSL se proporciona mediante certificados digitales. El certificado es un archivo que contiene determinada información de identificación. Un certificado se compra, o se recibe de otro modo, de una autoridad de certificación (CA) fiable. La principal responsabilidad de la CA es certificar la autenticidad de los usuarios.

Los certificados son archivos intransferibles y no falsificables que actúan como un tipo de identificador o pasaporte electrónico. Los certificados ayudan a asegurar que los usuarios o sistemas son quienes dicen ser. El archivo se firma con la clave privada de la CA para garantizar su autenticidad e integridad.

Un navegador habilitado por SSL utiliza el tipo de certificado conforme a los estándares del sector conocido como *X.509*. La versión 3 de X.509 contiene la siguiente información:

- Versión
- Número de serie
- ID de algoritmo de firma
- Nombre del emisor
- Periodo de validez
- Nombre del sujeto (usuario)
- Información de la clave pública del sujeto
- Identificador exclusivo del emisor (el nombre distinguido de la autoridad de certificación emisora)
- Identificador exclusivo del sujeto (el nombre distinguido del individuo que se identifica mediante el certificado)
- Extensiones (sólo para la Versión 3)
- Firmas para todos los campos indicados arriba

El estándar X.509 Versión 3 permite una información de identificación más detallada como, por ejemplo, en qué negocio está el poseedor del certificado y cuánto tiempo lleva en ese negocio. El emisor firma el certificado para autentificar el enlace entre el nombre del sujeto (usuario) y la clave pública del usuario.

Los certificados no prueban de forma concluyente que las personas o sistemas sean quienes dicen ser, pero indican que alguna CA tiene algún grado de confianza en la persona o el sistema. Cuando se confía en la CA que ha emitido el certificado, se tendrá un determinado grado de fiabilidad al intercambiar información con el poseedor del certificado.

Conceptos básicos del mecanismo de autentificación SSL

Un protocolo de *reconocimiento* SSL es el proceso en el que se intercambian señales para definir comunicaciones. El protocolo de reconocimiento SSL puede constar de dos fases:

- “Autentificación del servidor utilizando certificados del área del servidor” en la página 21
- “Autentificación del cliente utilizando certificados del área del cliente” en la página 21 (opcional)

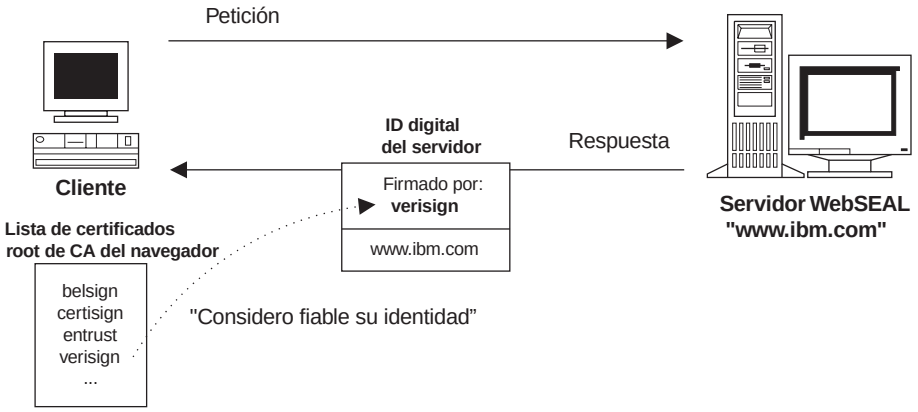
Tanto los clientes como los servidores pueden tener certificados. El servidor siempre debe tener un certificado para la autentificación a través de SSL. Los clientes pueden acceder al dominio seguro a través de SSL con o sin certificados del área del cliente.

Cuando un servidor envía su certificado a un cliente, el proceso se denomina *autentificación de servidor*. Cuando un cliente envía su certificado a un servidor, el proceso se denomina *autentificación de cliente*. La combinación de la autentificación del servidor y el cliente se conoce como *autentificación mutua*.

Autentificación del servidor utilizando certificados del área del servidor

Para una conexión SSL es necesaria la autentificación del servidor. La autentificación del servidor a través de SSL se lleva a cabo como sigue:

1. Un cliente solicita una conexión con un servidor habilitado para SSL.
2. En respuesta, el servidor firma (pero no cifra) su certificado. A continuación, el servidor envía al cliente el certificado que contiene la clave pública del servidor.
3. El cliente utiliza la clave pública del servidor incluida en el archivo del certificado para comprobar que el propietario del certificado es el mismo que lo firma.
4. El cliente comprueba si el emisor del certificado es uno de los que acepta buscando en la base de datos de certificados root de CA del navegador si existe la CA listada. Si es uno de los que acepta, el cliente va al siguiente paso; de lo contrario, el navegador informa al usuario de que el certificado lo emitió una CA desconocida. Entonces será responsabilidad del usuario el aceptar o rechazar el certificado.
5. El cliente genera a continuación una clave maestra, la cifra junto con la clave pública del servidor y transmite la clave maestra cifrada al servidor.
6. El servidor recupera la clave maestra y se autentifica ante el cliente devolviendo un mensaje que se cifra con la clave maestra. Los datos que siguen se cifran con claves que se derivan de esa clave maestra.



Autentificación del cliente utilizando certificados del área del cliente

El servidor desbloquea un certificado digital del cliente con la clave pública del cliente. Los certificados de clave pública tienen la sintaxis de X.509.

La autentificación utilizando certificados del área del cliente a través de SSL se lleva a cabo de la siguiente forma:

1. Cuando se ha completado la autentificación del servidor, éste envía una tentativa al cliente.
2. Tras la tentativa, el cliente devuelve su firma digital así como el certificado de clave pública. La firma digital se calcula utilizando la clave privada del cliente.
3. El servidor utiliza la clave pública del cliente incluida en el archivo del certificado para comprobar que el propietario del certificado es el mismo que lo firma.
4. El servidor intenta que el certificado coincida con una CA fiable. Si la CA del cliente no está listada como fiable, algunos servidores finalizan la transacción, anotan cronológicamente un error y devuelven un mensaje al cliente. Otros servidores pueden decidir proceder sin ese tipo de acción.
5. Cuando la CA del cliente se considera fiable, el servidor lleva a cabo la transacción.

Los certificados del área del cliente no son esenciales para la autentificación a través de una conexión SSL. La información cifrada podrá seguir intercambiándose. Los certificados de clientes proporcionan más seguridad al cliente y al servidor ya que aseguran el envío de la información cifrada a los destinatarios correctos. Es posible una autentificación mutua de fiabilidad con certificados de clientes.

En ambos casos, cuando el servidor CAS se ha definido para que requiera certificados de clientes para el control de accesos, los clientes se rechazarán si no tienen un certificado válido.

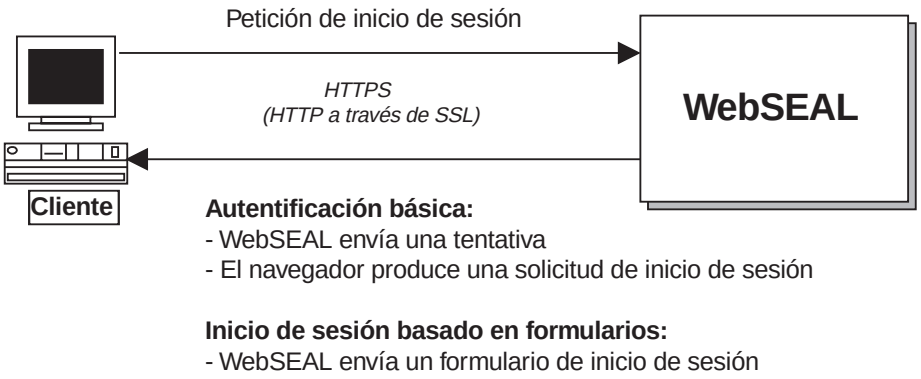
Para más información sobre los certificados X.509 del área del cliente utilizados por claves públicas y privadas, consulte el apartado “Método de autentificación de certificado X.509” en la página 175.

Autentificación de nombre de usuario y de contraseña

El proceso de autentificación requiere que el cliente presente algún tipo de información de identidad durante el inicio de sesión. Policy Director WebSEAL tiene soporte para la autentificación de nombre de usuario y contraseña.

Hay dos métodos de autentificación de nombre de usuario y contraseña que proporcionan esta información de identificación:

- Autentificación básica
- Inicio de sesión basado en formularios



En el apartado “Métodos de autentificación de nombre de usuario y de contraseña” en la página 171 encontrará toda la información sobre los mecanismos de autentificación que requieren información de identidad del cliente en forma de un nombre de usuario y una contraseña.

Autentificación de Kerberos

Kerberos Versión 5 es un protocolo de autentificación de la red que permite a dos partes autentificarse mutuamente para intercambiar información de forma segura a través de una red abierta.

Policy Director puede utilizar la autentificación de Kerberos en los siguientes intercambios:

- De Management Console a Management Server
- De Management Console a Security Server
- De Authorization Server a Management Server
- De WebSEAL a Management Server
- De WebSEAL a registro DCE (para autentificación de cliente)

Los servidores de Policy Director se comunican con otros servidores del dominio seguro de Policy Director utilizando Kerberos y el módulo de red del cliente NetSEAT. NetSEAT se comunica con el servicio de seguridad de Policy Director y define el túnel seguro de SSL durante el intercambio de información.

La autentificación de Kerberos depende de la fiabilidad fundamental de un tercero que responde de la veracidad de una o de las dos partes a autentificar. Este servicio de gestión de seguridad de un tercero fiable se denomina *servidor de seguridad (Security Server)*.

Policy Director Security Server (secd) es un servidor asegurado físicamente que almacena información relacionada con la seguridad (por ejemplo, nombres de usuarios, grupos y contraseñas) en una base de datos llamada *registro*.

Kerberos utiliza un mecanismo de clave secreta (LDAP Secret Key), compartido y específico de la sesión, para dar soporte a la autentificación mutua entre servidores. Kerberos cuenta con el Security Server fiable para la distribución de claves. El intercambio de información se lleva a cabo con Remote Procedure Call (RPC).

El protocolo de autentificación Kerberos es un complejo intercambio de una serie de mensajes. Dicho intercambio de mensajes contiene claves secretas y demás información necesaria para que los servidores puedan identificarse entre ellos. La finalidad de Kerberos es evitar que los participantes puedan conocer las claves de otros participantes. De hecho, la vida de muchas claves se limita a la duración de un solo intercambio.

Adquisición de credenciales

Una de las principales finalidades del proceso de autentificación es adquirir información de las credenciales que describa al usuario cliente. Policy Director diferencia la autentificación del usuario de la *adquisición de credenciales*.

La identidad de un usuario es siempre constante. Sin embargo, las credenciales que definen a los grupos o funciones en los que participa un usuario son variables. Las credenciales específicas del contexto pueden cambiar con el tiempo. Por ejemplo,

cuando se asciende a una persona, las credenciales deben reflejar el nuevo nivel de responsabilidad. Las credenciales de una persona en su trabajo también son diferentes de las credenciales de esa misma persona en su banco.

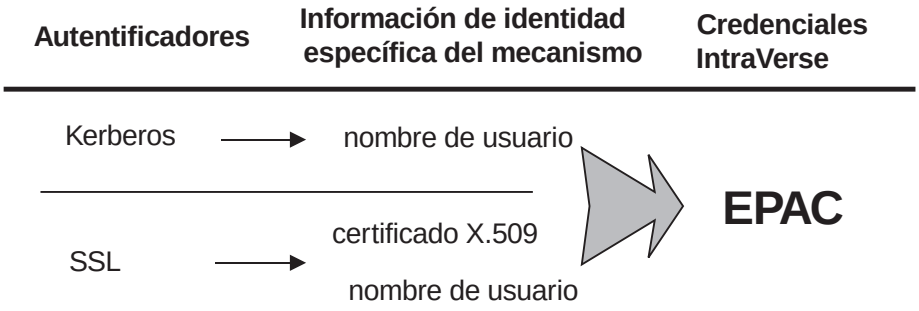
El proceso de autentificación tiene como resultado una información sobre la identidad del usuario específica del mecanismo. Después, esa información debe convertirse (*correlacionarse*) para adoptar una representación y un formato comunes para todo el dominio. Policy Director utiliza el formato EPAC.

Información sobre la identidad específica del mecanismo

Para un servicio de adquisición de credenciales, los distintos mecanismos de autentificación proporcionan distinta información de la identidad de los usuarios:

- Kerberos se basa en el nombre (y la contraseña) del usuario.
- Los certificados digitales X.509 del área del cliente proporcionan información de campo de X.509.
- Los métodos de inicio de sesión de autentificación básica y de autentificación basada en formularios (SSL) se basan en un nombre de usuario (y una contraseña).

La siguiente figura ilustra el tipo de información de identificación disponible desde el mecanismo de autentificación especificado y la utilización de un servicio de adquisición de credenciales a través de SSL para dar a la información el formato EPAC.



La información de identidad específica del mecanismo (por ejemplo, contraseñas, pares de claves y certificados) representa las propiedades de identidad físicas del usuario. Esta información se utiliza para establecer la sesión segura con el servidor.

La credencial resultante, que representa la función de un usuario en el dominio seguro, describe al usuario en un contexto específico y sólo es válida mientras dura la sesión.

Certificado EPAC

Cualquier servicio de Policy Director que necesite información acerca de un cliente utiliza credenciales. Por ejemplo, Policy Director Authorization Service utiliza credenciales para determinar si un usuario tiene autorización para realizar operaciones específicas en un recurso protegido del dominio seguro.

Una de las formas de trabajar con ACL es para que Policy Director utilice EPAC que contengan identificadores exclusivos universalmente (UUID). Policy Director utiliza credenciales para otros servicios como, por ejemplo:

- Auditing Service
- Posibilidades de delegación en conexiones (junction) WebSEAL y NetSEAL

Los siguientes campos del EPAC son adecuados para Policy Director:

Atributo	Descripción
ID de dominio seguro	Identificador de dominio seguro inicial del usuario
UUID de principal	UUID del usuario (o “principal” si DCE)
UUID de grupos	Uno o varios UUID de grupos a los que pertenece el usuario

La información de autentificación específica del mecanismo debe convertirse en campos EPAC:

- WebSEAL correlaciona automáticamente los clientes Policy Director con credenciales.
- Los clientes SSL procedentes de un registro externo que no sean de Policy Director, pueden correlacionar sus nombres de usuarios de un servicio de adquisición de credenciales externo.
- 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 un servicio de adquisición de credenciales externo.

Cadenas de fiabilidad

Durante el intercambio del protocolo SSL entre el cliente del navegador y el servidor WebSEAL, el servidor pasa al navegador una lista de certificados de las CA que el servidor considera fiables. Esto hace que el navegador muestre al usuario una lista de certificados del cliente del navegador que pueden:

- Estar firmados por una de las CA.
- Ser fiables gracias a una cadena de relaciones fiables con una de las CA que el servidor considere fiable—el certificado del cliente lo firma una CA en la cual la CA que efectúa la firma es considerada fiable por el servidor.

Este proceso se denomina *encadenamiento de certificados*.

El usuario del navegador selecciona uno de esos certificados de cliente para efectuar la transmisión al servidor. Si el certificado del cliente esta firmado directamente por una de las CA que el servidor considera fiables, el navegador transmitirá únicamente el certificado del cliente al servidor (suponiendo que el servidor tenga ya el certificado de la CA que efectúa la firma.

Si el certificado del cliente no lo ha firmado directamente una de las CA que el servidor considera fiable, el navegador crea y transmite una cadena de certificados que ilustra la cadena de fiabilidad entre el certificado del cliente una de las CA que el servidor considera fiable.

De nuevo, el navegador no transmite realmente el certificado de la CA que el servidor considera fiable. Supone que el servidor ya tiene el certificado.

El archivo de configuración secmgrd.conf de Policy Director contiene una lista de certificados root de la CA que Policy Director considera fiables. Por lo tanto, Policy Director considera fiables los certificados de clientes emitidos por dichas CA.

El servidor toma cada certificado de CA transmitido por el navegador y comprueba:

- Si el certificado es un certificado de CA.
- La firma de la CA que estampa la firma.
- Si el certificado no ha caducado.

Una *cadena de fiabilidad* se considera establecida cuando una CA considera fiable una segunda CA, que considera fiable una tercera CA, y así sucesivamente. Si Policy Director considera fiable cualquiera de las CA de esta cadena de fiabilidad, debería considerar fiable el certificado del cliente.

Visión general del servicio de adquisición de credenciales

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*.

Cualquier servicio de Policy Director que necesite información acerca de un cliente utiliza la credenciales que se derivan del proceso de autentificación. Entre estos servicios se incluyen el de autorización y el de auditoría. Las principales funciones de Policy Director dependen de la disponibilidad de las credenciales para cada cliente.

Policy Director utiliza el formato EPAC para representar la información de credenciales que se deriva del proceso de autentificación.

Policy Director genera automáticamente credenciales para los clientes SSL que:

- Sean miembros del dominio seguro.
- Estén autentificados con un nombre de usuario y una contraseña válidos.

En ese caso, el nombre de usuario y la contraseña proporcionados deben coincidir con una entrada de cuenta existente en el registro por omisión (LDAP).

Hay otros posibles supuestos en los que el acceso del cliente no se ajusta al modelo indicado arriba:

- El cliente no pertenece al registro por omisión de Policy Director.
- El acceso del cliente se efectúa utilizando el certificado del área del cliente.

En los tres casos, Policy Director debe confiar en una autentificación personalizada y en un servicio de correlación que pueda:

- Efectuar la autentificación en dichos clientes.
- Hacer referencia a un registro de cuentas externo (de terceros).
- Correlacionar la información de identidad externa con un identidad de Policy Director.

Esta autentificación personalizada y el servicio de correlación se conocen como *servicio de adquisición de credenciales externo* (CAS).

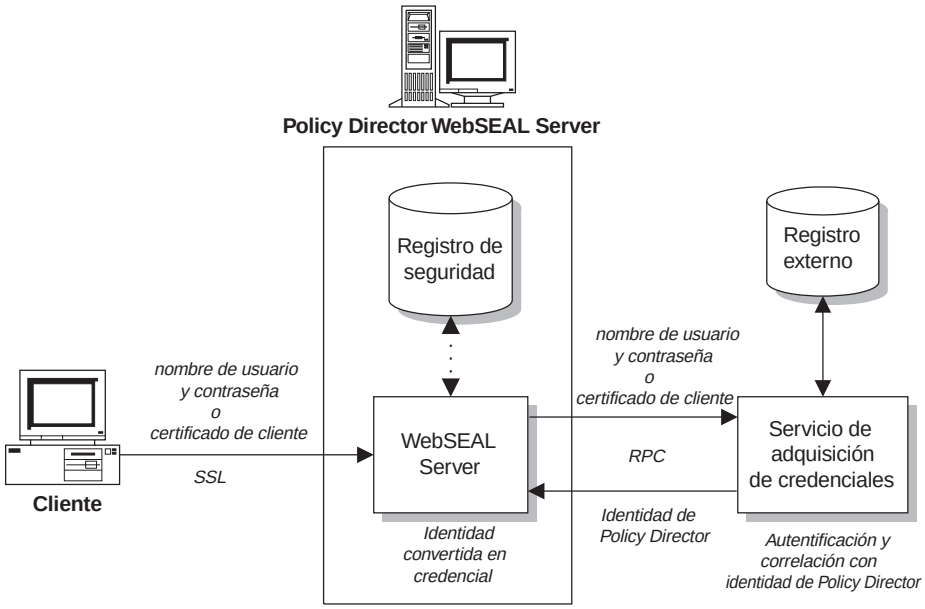
Presentación del servicio de adquisición de credenciales

La arquitectura de un servicio de adquisición de credenciales (CAS) permite sustituir el proceso de autentificación de WebSEAL SSL por omisión (que se basa en un nombre de usuario y una contraseña) por un proceso de autentificación externo personalizado que puede hacer referencia a un registro de usuario que no sea el registro de seguridad de Policy Director. El servicio de adquisición de credenciales personalizado efectúa también la correlación adecuada de cualquier información de identidad especial (certificados, señales) con una identidad de Policy Director.

El administrador debe escribir y personalizar especialmente el servicio de adquisición de credenciales para que proporcione una solución específica para el dominio seguro.

El servicio de adquisición de credenciales debe utilizar interfaces RPC para asegurar todas las comunicaciones entre WebSEAL y el servidor CAS.

Un servicio de adquisición de credenciales permite que un usuario que no tenga una cuenta en el registro de Policy Director por omisión participe del dominio seguro. El servicio de adquisición de credenciales puede autentificar a dicho usuario (utilizando un registro externo si es necesario). A continuación, el servicio de adquisición de credenciales devolverá una identidad de Policy Director a WebSEAL para que la convierta en credenciales. Policy Director utiliza esas credenciales para permitir que el usuario participe del dominio seguro.



Un servicio de adquisición de credenciales puede acomodar bases de datos de usuarios antiguas que sería difícil o imposible migrar al registro que utiliza normalmente Policy Director. Un ejemplo de sistema antiguo podría incluir un ID de cliente y un mecanismo de PIN (señal). Un mecanismo antiguo de autentificación de este tipo comprueba la información del usuario mediante su propia base de datos de registros.

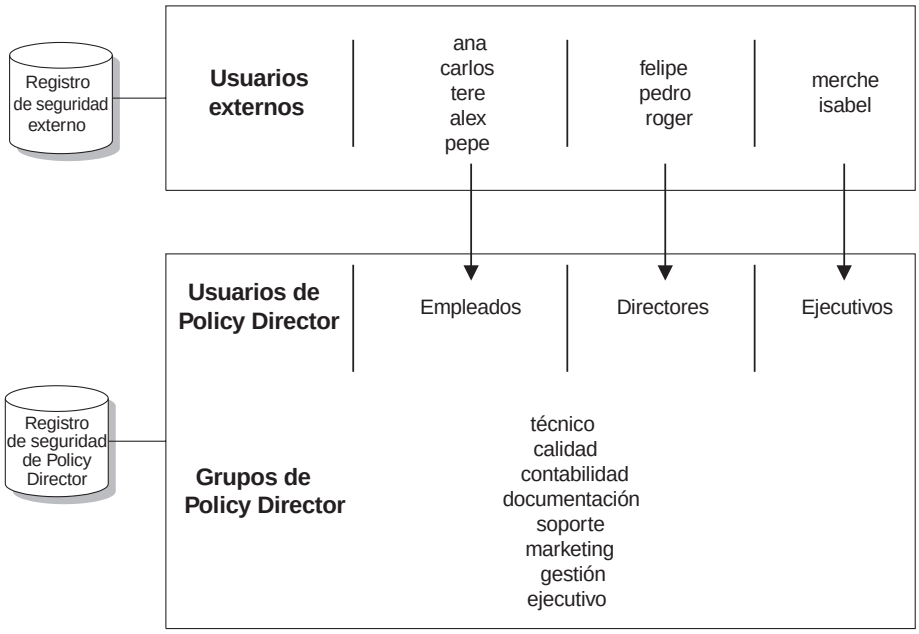
Policy Director Authorization Application Developer's Kit (IVAuthADK) facilita un servidor CAS de demostración. Este servidor define la interfaz (un IDL) entre WebSEAL y el servicio de adquisición de credenciales. El ADK también proporciona código fuente por si se escribe un servicio de adquisición de credenciales propio.

Solución de correlación multívoca

Un servicio de adquisición de credenciales es adecuado para una solución *multívoca*; es decir, que el módulo permite correlacionar muchas cuentas antiguas con un usuario de Policy Director.

En la correlación multívoca, un usuario de Policy Director asume la función de un grupo cuyos miembros son el grupo de usuarios de la base de datos antigua. La solución de correlación multívoca da como resultado idénticos derechos de acceso, visibilidad y contabilidad para todos los usuarios correlacionados con un mismo usuario. Todos los usuarios correlacionados con un usuario determinado tienen exactamente los mismos permisos. Este hecho debe tenerse en cuenta para determinar la política de seguridad.

En la siguiente figura, los usuarios de un registro externo podrían correlacionarse con un solo usuario de Policy Director. Por ejemplo, el usuario de Policy Director (`Empleados`) actúa como función para un grupo de usuarios del registro externo. Aunque los usuarios se correlacionan con la misma cuenta de Policy Director, también pueden distinguirse individualmente al asignárseles la pertenencia a uno o más grupos de Policy Director. Las decisiones de autorización de Policy Director pueden basarse en la identidad y la pertenencia del usuario a un grupo.



Nota: El nivel de contabilidad de una correlación multívoca no es estricto. Los servicios de auditoría (Auditing Services) sólo efectúan un seguimiento del usuario de Policy Director—no de los usuarios individuales correlacionados con ese usuario.

Modalidades de función

Un servicio de adquisición de credenciales puede escribirse para que procese información de autentificación como, por ejemplo, certificados de clientes, nombres de usuarios y señales. Deberá configurar WebSEAL para que acepte clientes que no sean del registro de SSL y direccionar la información de autentificaciones al servicio de adquisición de credenciales adecuado para que efectúe la autentificación y la correlación con una identidad de Policy Director.

Un servicio de adquisición de credenciales realiza la autentificación y correlación de identidades basándose en la información de identidad específica proporcionada por el cliente. Por lo tanto, el servicio de adquisición de credenciales puede escribirse para que se ejecute en una de las siguientes modalidades:

- “Modalidad de correlación de certificado X.509”
- “Modalidad de correlación de nombre de usuario” en la página 31

En el apartado “Servicio de adquisición de credenciales personalizado” en la página 34 encontrará información sobre la utilización de servicios de adquisición de credenciales escritos por usuarios.

Modalidad de correlación de certificado X.509

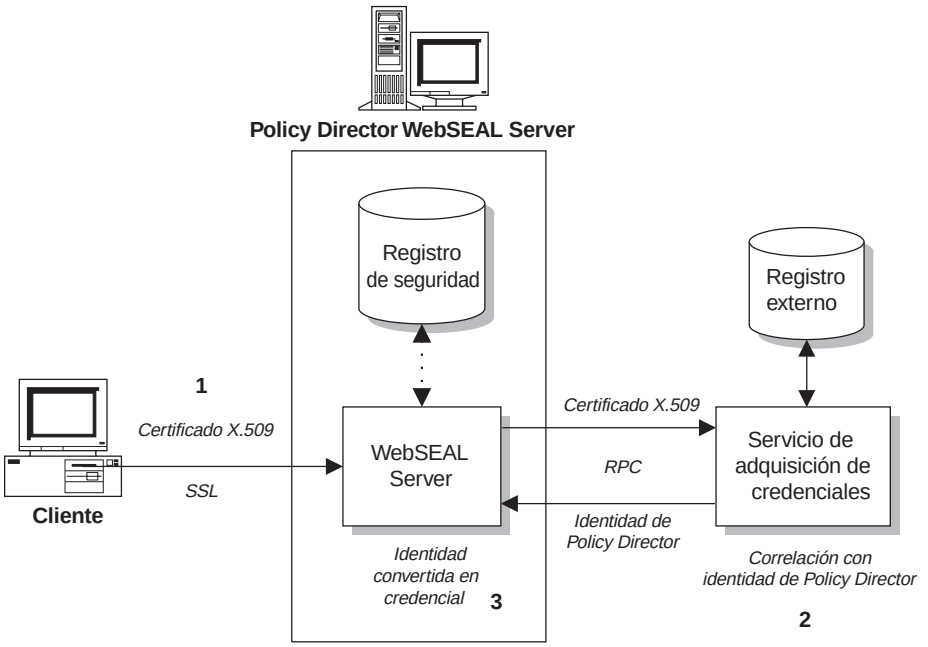
A través del servicio de adquisición de credenciales, Policy Director puede soportar la autentificación de clientes que utilicen certificados digitales X.509 a través de SSL. Una modalidad X.509 del servicio de adquisición de credenciales correlaciona información específica incluida en un certificado digital X.509 del área del cliente con una identidad de Policy Director. Esta identidad de Policy Director se devuelve a WebSEAL, que la convierte en las credenciales adecuadas.

La modalidad X.509 es adecuada en las siguientes condiciones:

1. Los clientes se comunican a través de SSL.
2. Los clientes utilizan certificados digitales X.509 para la autentificación.
3. Los clientes deben acceder a recursos protegidos del dominio seguro Policy Director.

Un servidor CAS puede correlacionar la información del certificado con una identidad de Policy Director sobre una base biunívoca o multívoca. La finalidad del servicio de correlación es proporcionar a Policy Director Authorization Service credenciales útiles para la toma de decisiones de autorización.

La siguiente figura ilustra la secuencia de sucesos que se producen cuando WebSEAL se ha configurado para que utilice un servicio de adquisición de credenciales para la correlación de certificados X.509.



1. El cliente accede a WebSEAL a través de SSL y presenta un certificado X.509.

   Tenga en cuenta que, al llegar a este punto, la autentificación se lleva a cabo a través de un intercambio de certificados de clave pública y privada. La única

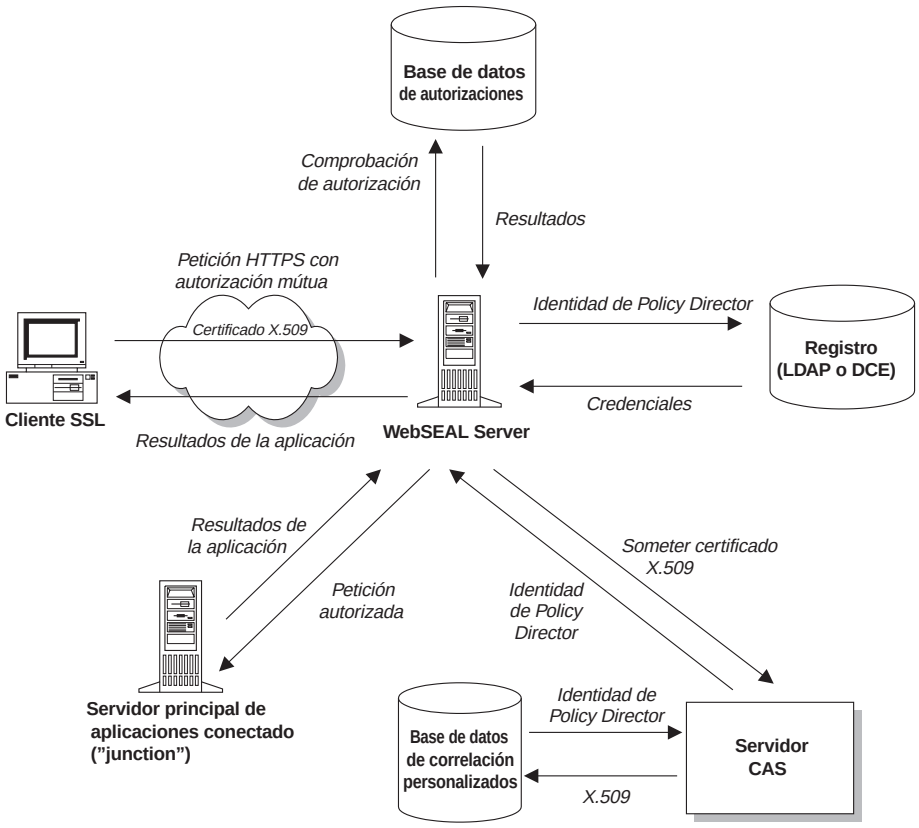
función que queda para el servicio de adquisición de credenciales es correlacionar las credenciales de usuario.

2. El servidor CAS toma información de una identidad (específica de la aplicación) en el certificado validado y la correlaciona con una identidad conocida por Policy Director. El servidor CAS puede utilizar un registro externo (de terceros).
3. La identidad de Policy Director se devuelve a WebSEAL que utiliza después su registro por omisión para convertir la identidad en las credenciales correspondientes.

Utilización de un servicio de adquisición de credenciales en modalidad X.509

La siguiente figura ilustra la secuencia completa de sucesos que se producen cuando un cliente, que accede a WebSEAL utilizando un certificado X.509, solicita un recurso del dominio seguro.

1. La información del certificado se correlaciona con una identidad de Policy Director a través del servicio de adquisición de credenciales, que devuelve la identidad a WebSEAL.
2. WebSEAL crea una credencial a partir de esa identidad y la utiliza para tomar la decisión de autorización que implica a un recurso protegido de un servidor de aplicaciones conectado (junction).



Modalidad de correlación de nombre de usuario

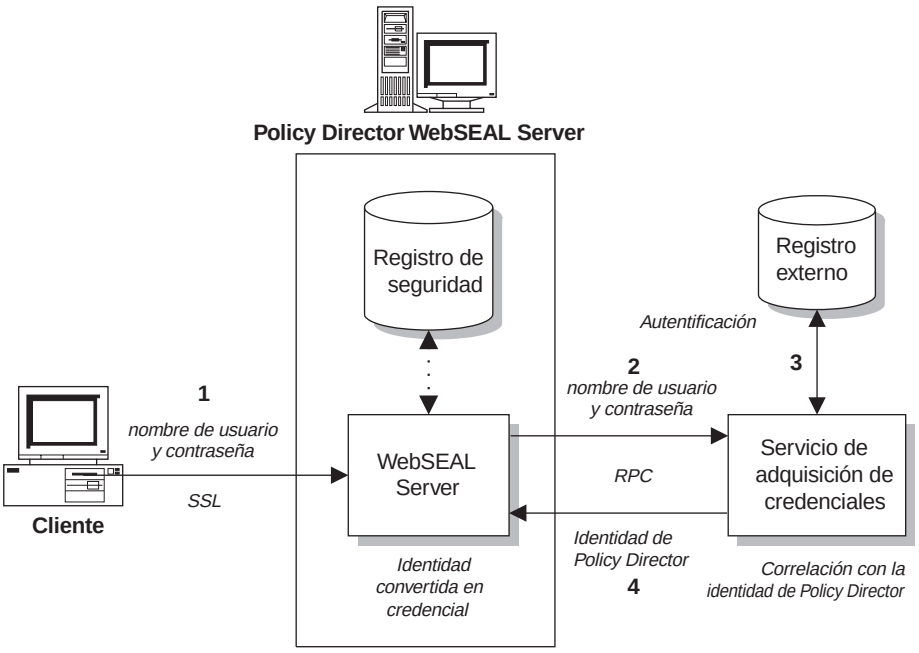
La modalidad de correlación de nombre de usuario es otro tipo de autentificación y correlación de identidades. Utilizando la modalidad de correlación de nombres de usuario, se puede sustituir el proceso de autentificación por omisión por un proceso externo que haga referencia a un registro de usuarios distinto del registro por omisión de Policy Director (LDAP).

La autentificación estándar de Policy Director utilizando SSL requiere que el usuario inicie la sesión con un nombre de usuario y una contraseña. La autentificación y la adquisición de credenciales para esa identidad se determinan en el registro de Policy Director.

La principal utilidad de un servicio de adquisición de credenciales es acomodar las bases de datos de usuarios antiguas que sería difícil o imposible migrar al registro de Policy Director.

La siguiente figura ilustra la secuencia de sucesos que se producen cuando WebSEAL se ha configurado para que utilice un servicio de adquisición de credenciales para la correlación de nombres de usuarios:

1. El cliente accede a WebSEAL a través de SSL con un nombre de usuario y una contraseña.
2. WebSEAL se configura para pasar nombres de usuarios y contraseñas al servicio de adquisición de credenciales tanto para la autentificación como para la adquisición de credenciales.



3. El servicio de adquisición de credenciales utiliza un registro externo (de terceros) para autentificar al usuario y después correlaciona dicho usuario con una identidad de Policy Director.
4. La identidad de Policy Director se devuelve a WebSEAL que utiliza después su registro por omisión para convertir la identidad en una credencial.

Esta modalidad se utiliza mejor como solución multívoca; es decir, que el módulo permite correlacionar muchas cuentas antiguas con un usuario de Policy Director. Consulte el apartado “Solución de correlación multívoca” en la página 27.

Opciones del servicio de autentificación

Puede elegir uno de los siguientes tipos de servicio de autentificación:

- El servicio Policy Director Credentials Acquisition Service por omisión (consulte el apartado “CAS proporcionado por Policy Director”).
- Un servicio de adquisición de credenciales escrito por el cliente (consulte el apartado “Servicio de adquisición de credenciales personalizado” en la página 34).

CAS proporcionado por Policy Director

Policy Director proporciona un componente propio de autentificación de clientes, Policy Director Credentials Acquisition Service (Policy Director CAS). Policy Director CAS puede utilizarse cuando se emplea LDAP como registro de usuarios.

Debe configurar WebSEAL para que utilice Policy Director CAS para la autentificación comprobando y actualizando los archivos de configuración iv.conf y secmgrd.conf (consulte el apartado “Configuración de Policy Director Credentials Acquisition Service” en la página 177).

Policy Director CAS correlaciona *certificados digitales de clientes* procedentes del navegador habilitado para SSL con una identidad de usuario de Policy Director. Cuando el usuario intenta acceder a una página 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. Policy Director CAS intenta correlacionar el certificado que ha recibido con una identidad de usuario que Policy Director pueda entender.

Policy Director Credentials Acquisition Service se ha escrito para proporcionar soporte para el inicio de sesión a través de SSL utilizando uno o los dos certificados X.509 Versión 3 del área del cliente:

- Producto conforme a las normas PKIX (por ejemplo, IBM SecureWay Trust Authority, Versión 3.1)
- Producto conforme a las normas Entrust (por ejemplo, IBM Vault Registry, Versión 2.2.2)

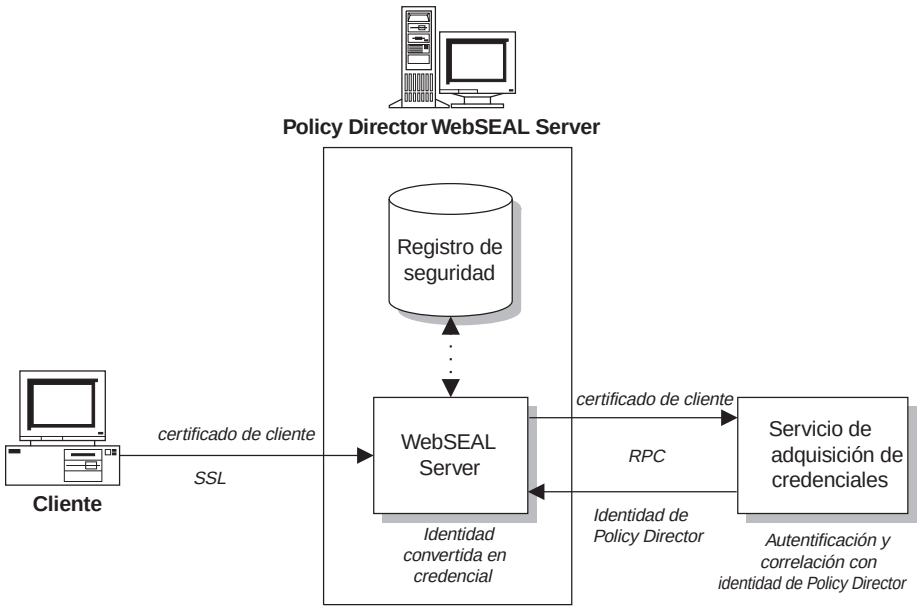
Todos los certificados están codificados con Distinguished Encoding Rules (DER) cuando se transmiten.

Entre Policy Director Credentials Acquisition Service y WebSEAL se utiliza una interfaz RPC. Policy Director Credentials Acquisition Service utiliza interfaces RPC para asegurar todas las comunicaciones entre WebSEAL y el servidor CAS. Como Policy Director Credentials Acquisition Service es una aplicación DCE-RPC, es necesario un cliente DCE para efecturar la correlación correspondiente de identidad del cliente.

El servicio Policy Director Credentials Acquisition Service por omisión:

- Permite utilizar certificados del área del cliente o especificar que son opcionales.

- No efectúa ninguna comprobación de lista de revocación de certificados (CRL) asociada.
- Soporta el encadenamiento de certificados.
- Tiene soporte para la solución de correlación biunívoca.



Solución de correlación biunívoca

Policy Director Credentials Acquisition Service utiliza la modalidad de correlación biunívoca. Una correlación *biunívoca* de cuentas antiguas individuales con usuarios individuales puede requerir un alto grado de mantenimiento de la contabilidad. Sin embargo, dentro del archivo de configuración cdas.conf de Policy Director CAS, el administrador de Policy Director puede crear una tabla que se utilice para asociar un nombre distinguido (DN) de certificado con el DN de un usuario de Policy Director.

Cuando WebSEAL llama a Policy Director CAS con un certificado, primero extrae el DN del certificado y comprueba si hay alguna coincidencia en la tabla. Si encuentra una coincidencia, Policy Director Credentials Acquisition Service devuelve a WebSEAL el DN del usuario asociado de Policy Director formateado correctamente. WebSEAL utiliza entonces ese DN para identificar al usuario de Policy Director (LDAP). 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 (LDAP). WebSEAL Server usa el DN devuelto para recuperar las credenciales del usuario.

Tareas de administración necesarias

Las tareas de administración necesarias para configurar el servicio Policy Director Credentials Acquisition Service son, entre otras:

1. Configurar WebSEAL para que utilice CAS para la autentificación comprobando y actualizando, si es necesario, los archivos de configuración iv.conf y secmgrd.conf (consulte el apartado “Configuración de Policy Director Credentials Acquisition Service” en la página 177).
2. Si es necesario, actualizar la sección de la tabla de correlación de DN del archivo de configuración cdas.conf (consulte el apartado “Correlación de nombres distinguidos” en la página 178).

Funcionalidad de Credentials Acquisition Service

La interfaz de Policy Director Credentials Acquisition Service puede utilizarse para proporcionar las siguientes funciones:

- WebSEAL llama a Policy Director CAS con un certificado.
- Policy Director CAS extrae el DN del certificado y comprueba si hay alguna correlación de DN en la tabla de correlaciones de DN.
- Si se encuentra una coincidencia:
  - Policy Director Credentials Acquisition Service devuelve a WebSEAL el DN del usuario asociado de Policy Director.
  - WebSEAL utiliza entonces ese DN para identificar al usuario de Policy Director.
- Si no se encuentra ninguna coincidencia:
  - CAS devuelve el DN del certificado a WebSEAL.
  - 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.

Servicio de adquisición de credenciales personalizado

Debido a la diversidad de cada servidor de aplicaciones y a la infraestructura de autentificación correspondiente, es imposible escribir ningún servicio de adquisición de credenciales que satisfaga todas las necesidades. Por este motivo, con Policy Director se incluye el código fuente de servidor CAS de demostración en el paquete IVAuthADK. Dicho servidor CAS de demostración puede adoptarse como infraestructura básica para un servidor CAS de producción—añadiéndole las funciones de correlación de nombres de usuarios y de gestión de correlaciones específicas de la aplicación.

Deberá configurar WebSEAL para que acepte clientes que no sean del registro de SSL y direccionar la información de autentificaciones al servicio de adquisición de credenciales adecuado para que efectúe la autentificación y la correlación con una identidad de Policy Director.

El servicio CAS debe utilizar interfaces RPC para asegurar todas las comunicaciones entre WebSEAL y el servidor CAS.

Los requisitos para correlacionar información de certificados X.509 con una identidad de Policy Director varían mucho según los clientes. Aunque Policy Director no incluye ninguna norma genérica para definir un servicio de correlación, se proporcionan dos elementos que ayudarán al administrador que desee escribir un servicio de correlación personalizado:

1. Policy Director define una interfaz de IDL que permite a los programadores escribir un servicio propio que correlacione información de certificados X.509 con identidades de Policy Director. En el manual *Policy Director Programmer's Guide and Reference* encontrará detalles sobre esta interfaz de IDL.
2. Policy Director incluye un ejemplo de implementación de un servicio de correlación que proporciona una infraestructura de servidor CAS que simplemente devuelve un error para cada petición. Esta infraestructura puede desarrollarse más ampliamente en un servidor CAS de producción.

   El código fuente del servicio de ejemplo está incluido en el paquete de instalación IVAuthADK de Policy Director.

Tareas de administración necesarias

Las tareas de administración necesarias para configurar un CAS personalizado son, entre otras:

1. Escribir un CAS personalizado que utilice la interfaz de IDL proporcionada por Policy Director.
2. Configurar WebSEAL para que utilice el servicio de adquisición de credenciales externo para la autentificación.

Funcionalidad del CAS personalizado

La interfaz del CAS personalizado puede utilizarse para obtener las siguientes funciones:

- Efectuar la validación del nombre de usuario y la contraseña con un registro de usuarios que no sea el registro de Policy Director por omisión.
- Correlacionar muchos usuarios con la misma identidad de Policy Director.
- Gestionar contraseñas de usuarios externos.
- Añadir a la credencial información de auditoría del cliente. Policy Director graba toda la credencial en el archivo de anotaciones cronológicas de auditoría.

Capítulo 3. Qué es una autorización

Una *autorización* es un proceso que determina si una entidad identificada tiene derecho o autorización para:

- Iniciar un servicio específico.
- Realizar una operación sobre un recurso específico de un dominio seguro.

Policy Director Authorization Service ayuda a poner en vigor la política de seguridad de una red controlando el proceso de toma de decisiones de autorización.

Este capítulo incluye los siguientes temas:

Modelo conceptual de autorización

Cuando los servidores ponen en vigor la seguridad en un dominio seguro, cada cliente debe proporcionar una prueba de su identidad. A su vez, la política de seguridad determina si el cliente tiene permiso para realizar una operación sobre un recurso solicitado. El servidor controla el acceso a cada recurso de un dominio seguro. Por este motivo, las demandas de autentificación y autorización del servidor pueden proporcionar una amplia seguridad en la red.

La *autentificación* es el proceso en el que se identifica a un individuo que intenta iniciar la sesión con un dominio seguro.

En los sistemas de seguridad, la autentificación es distinta de la autorización:

- La *autentificación* es el proceso en el que se identifica a un individuo que intenta iniciar la sesión con un dominio seguro. La autentificación asegura que los individuos sean quienes dicen ser, pero no dice nada acerca de los derechos para realizar operaciones en un recurso protegido.
- La *autorización* determina si un cliente autentificado tiene derechos para realizar una operación en un recurso específico de un dominio seguro. En el modelo de autorización, Policy Director lleva a cabo la política de autorización independientemente del mecanismo que se utiliza para la autentificación del usuario. Los usuarios pueden autentificar su identidad utilizando una clave pública/privada, una clave secreta o mecanismos definidos por el cliente.

Parte del proceso de autentificación implica la adquisición de una credencial que describa la identidad del cliente. Un servicio de autorizaciones basa sus decisiones en cuanto a autorizaciones en las credenciales de los usuarios.

Los recursos de un dominio seguro reciben un nivel de protección dictado por la política de seguridad de dicho dominio. La política de seguridad define los usuarios autorizados a participar en el dominio seguro y el grado de protección rodeando cada recurso que requiera protección.

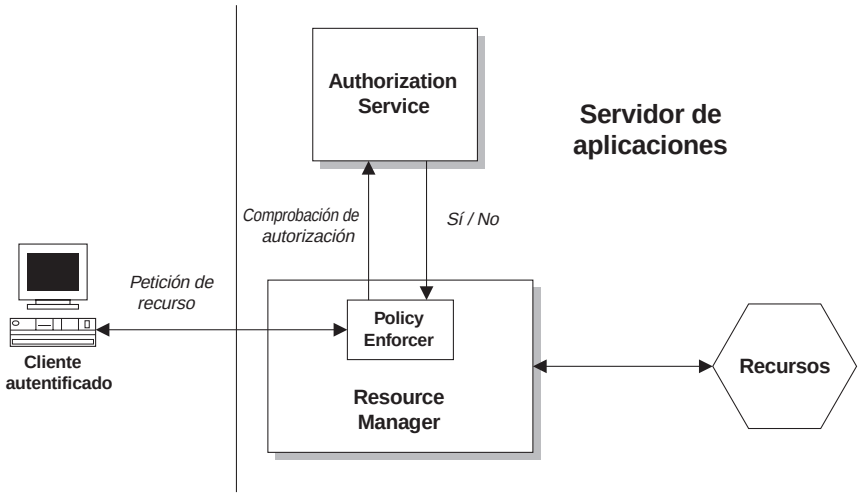
Los componentes básicos del proceso de autorizaciones son, entre otros:

Resource Manager

El gestor de recursos (Resource Manager) es responsable de llevar a cabo la operación solicitada cuando Policy Director otorga la autorización. Uno de los componentes del gestor de recursos es Policy Enforcer que dirige la petición al servicio de autorizaciones para su proceso.

Authorization Service

El servicio de autorizaciones (Authorization Service) realiza la acción de toma de decisión para la petición.



Las aplicaciones tradicionales unen Policy Enforcer y Resource Manager en un proceso. Ejemplos de esta estructura serían Policy Director WebSEAL y aplicaciones de terceros. La funcionalidad independiente de estos componentes de autorización permite más flexibilidad en el diseño de la estrategia de aplicación de la seguridad.

Una independencia de este tipo permite, por ejemplo, que el administrador de seguridad controle:

- La ubicación de los procesos.
- La persona que escribe el código de los procesos.
- La forma en que los procesos realizan sus tareas.

Ventajas de un servicio de autorizaciones estándar

En la mayoría de sistemas, tanto antiguos como nuevos, la autorización está estrechamente ligada a aplicaciones individuales. Normalmente, las empresas crean con el tiempo aplicaciones que se adaptan a sus necesidades. Muchas de esas aplicaciones requieren alguna forma de autorización específica.

El resultado es frecuentemente una amplia variedad de aplicaciones con distintas implementaciones de autorización. Dichas implementaciones de autorización propias requieren una administración separada, son difíciles de integrar y acaban produciendo mayores costes de explotación.

Un servicio de autorizaciones distribuido puede proporcionar a las aplicaciones independientes un mecanismo estándar de toma de decisiones sobre autorizaciones.

Un servicio de autorizaciones estándar tiene las siguientes ventajas:

- Reduce el coste de desarrollar y gestionar el acceso a aplicaciones.
- Reduce el coste total de explotación y gestión de distintos sistemas de autorizaciones .
- Potencia la infraestructura de seguridad existente.
- Permite una apertura más segura de nuevos negocios.
- Permite habilitar más aplicaciones nuevas y de distintos tipos.
- Permite que los ciclos de desarrollo sean más cortos.
- Comparte la información de forma segura.

Ventajas de Policy Director Authorization Service

Policy Director se integra tanto en las infraestructuras antiguas ya existentes como en las nuevas. Policy Director permite una gestión de política centralizada y segura. Policy Director Authorization Service—junto con los gestores de recursos de WebSEAL y NetSEAL—proporciona un mecanismo de autorización estándar para sistemas comerciales de la red.

Las aplicaciones existentes pueden beneficiarse del servicio de autorizaciones sin necesidad de modificar la aplicación propiamente dicha. Policy Director basa su política de autorizaciones en las funciones de usuarios o de grupos. Las políticas de autorizaciones pueden aplicarse a:

- Servidores de red
- Transacciones individuales o peticiones de la base de datos
- Información específica basada en la Web
- Actividades de gestión
- Objetos definidos por el usuario

La API de autorizaciones de Policy Director permite que aplicaciones existentes efectúen llamadas a Policy Director Authorization Service. A su vez, el servicio de autorizaciones toma decisiones basándose en la política de seguridad de la empresa. Consulte el apartado “API de autorizaciones de Policy Director” en la página 48.

Policy Director Authorization Service también es ampliable. Policy Director Authorization Service puede configurarse para que llame a otros servicios de autorizaciones para efectuar procesos suplementarios utilizando la API de autorizaciones externa de Policy Director.

Policy Director Authorization Service tiene las siguientes ventajas:

- No depende de las aplicaciones.
- Utiliza un tipo de codificación de autorizaciones independiente del lenguaje (la API de autorizaciones de Policy Director).
- Se gestiona centralmente y, por lo tanto, es fácil de administrar. Por ejemplo, para añadir un nuevo empleado deberá modificarse la base de datos de privilegios en una ubicación central y no en varios sistemas.
- Dirige la aplicación de los servicios de seguridad en un entorno heterogéneo de varias plataformas.
- Integra sistemas de autorizaciones que no son de Policy Director mediante una función de servicio de autorizaciones externo.
- Tiene una arquitectura flexible y escalable que se integra con facilidad en la infraestructura existente.

- Permite la autorización a varios niveles—el servicio pasa un paquete de credenciales a través de múltiples capas de un proceso de aplicación o transacción.
- Utiliza un modelo de auditoría común y efectivo.
- Es independiente de cualquier mecanismo de autentificación.

Policy Director Authorization Service

Policy Director Authorization Service es responsable del proceso de toma de decisiones de autorización que ayuda a instaurar una política de seguridad de red. Las decisiones de autorización tomadas por el servicio de autorizaciones tienen como resultado la aprobación o denegación de las peticiones de clientes que desean realizar operaciones en recursos protegidos del dominio seguro.

Componentes de Policy Director Authorization Service

Tres componentes básicos forman Policy Director Authorization Service:

- La base de datos primaria (maestra) de políticas de autorización
- El Management Server
- El evaluador de toma de decisiones de autorización

Base de datos maestra de políticas de autorización

La base de datos primaria de políticas de autorización contiene la información de políticas de seguridad para todos los recursos del dominio seguro. La base de datos también contiene toda la información necesaria de credenciales asociada a los miembros del dominio seguro.

Para entrar y cambiar los contenidos de esta base de datos se utiliza Policy Director Management Console.

Management Server

Management Server (ivmgrd) realiza las siguientes tareas:

- Mantiene la base de datos de políticas de autorización.
- Reproduce esa información sobre políticas en todo el dominio seguro.
- Actualiza las réplicas de la base de datos siempre que se efectúa un cambio en la base de datos de políticas de autorización.

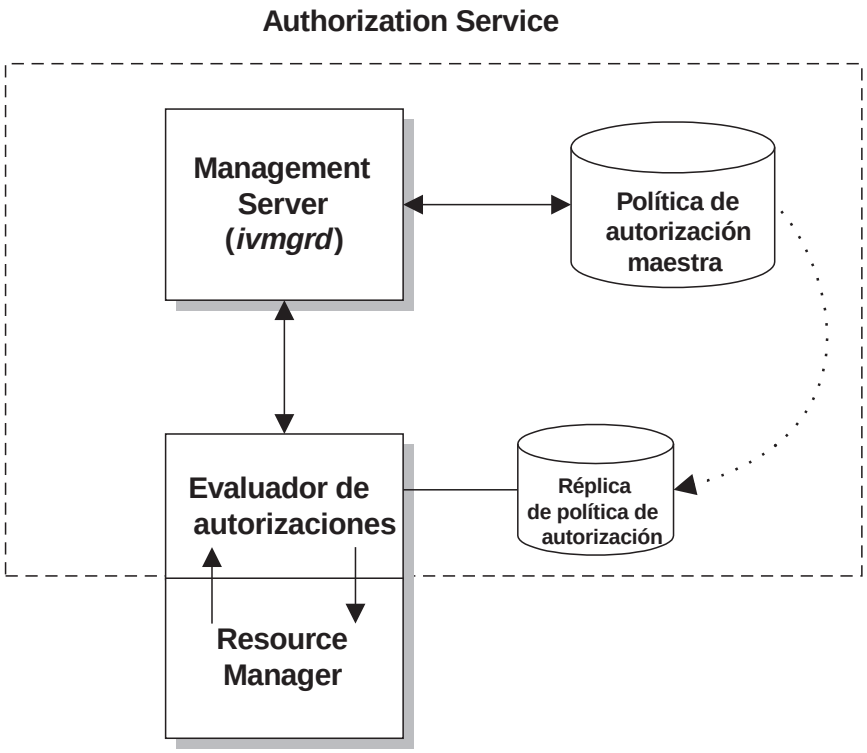
Management Server también mantiene la información de las ubicaciones de otros servidores que estén operando en el dominio seguro, sean o no de Policy Director.

Nota: Debe haber una sola instancia de Management Server en cualquier dominio seguro.

Evaluador de autorizaciones

El evaluador de autorizaciones es el proceso de toma de decisiones que determina la posibilidad de acceso de un cliente a un recurso protegido, basado en la política de seguridad. El evaluador pasa su recomendación al gestor de recursos que, a su vez, responde en consecuencia.

La siguiente figura ilustra los principales componentes de Policy Director Authorization Service:



Interfaces de Policy Director Authorization Service

Policy Director Authorization Service tiene dos interfaces en las que se lleva a cabo la interacción:

Interfaz de gestión

El administrador de seguridad gestiona la política de seguridad en la red. El administrador de seguridad utiliza Policy Director Management Console o el programa de utilidad **ivadmin** para:

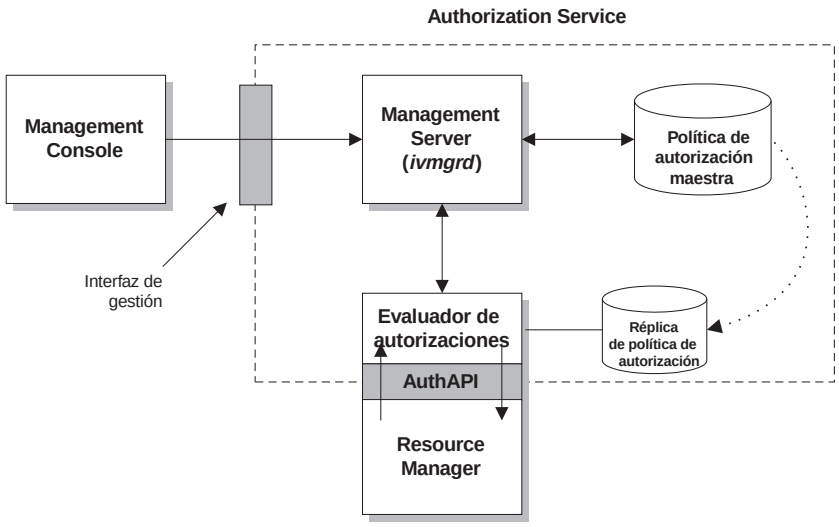
- Aplicar normas (plantillas) de políticas en los recursos de la red.
- Registrar las credenciales de los participantes en el dominio seguro.

Management Console aplica estos datos de políticas de seguridad a la base de datos primaria de políticas de autorización que utiliza Management Server.

Esta interfaz implica un conocimiento detallado del espacio de nombres, las plantillas de las políticas y las credenciales.

API de autorizaciones

La API de autorizaciones de Policy Director pasa las peticiones de decisiones de autorización desde el gestor de recursos al evaluador de autorizaciones que devuelve entonces una recomendación. El manual *Policy Director Programmer's Guide and Reference* contiene información detallada sobre esta API.



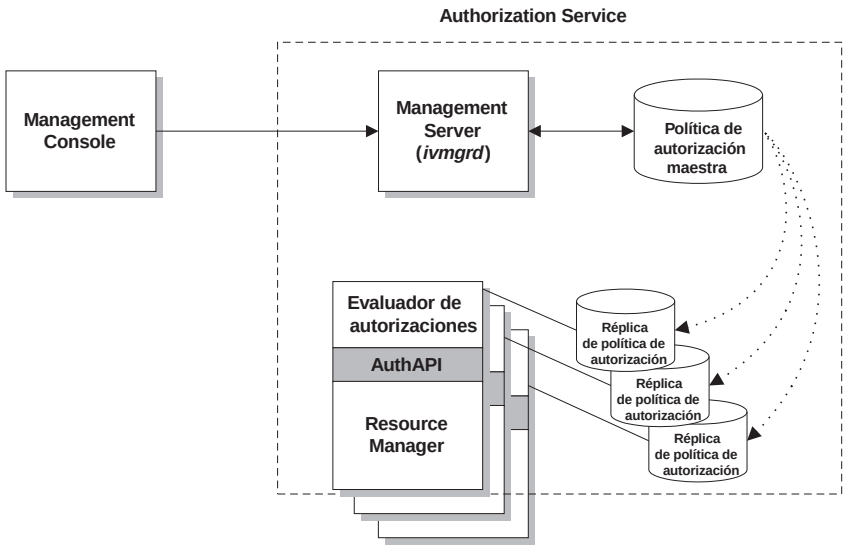
Reproducciones para la escalabilidad y el rendimiento

Los componentes de Policy Director Authorization Service pueden reproducirse para aumentar su disponibilidad en un entorno que tenga una demanda alta.

Policy Director reproduce siempre automáticamente la base de datos primaria de políticas de autorización que contiene las normas de las políticas e información sobre credenciales. Las aplicaciones que llaman al servicio de autorizaciones tienen dos opciones para hacer referencia a esta información de la base de datos:

- La aplicación, cuando se ha configurado para funcionar sin problemas con el evaluador de autorizaciones, utiliza una antememoria local de la base de datos. La reproducción de la base de datos se lleva a cabo para cada aplicación que utilice el servicio de autorizaciones en modalidad de antememoria local.
- La aplicación utiliza una réplica compartida colocada en la antememoria por el componente Policy Director Authorization Server remoto. La reproducción de la base de datos se lleva a cabo para cada instancia de Policy Director Authorization Server. Varias aplicaciones pueden acceder a un solo Authorization Server.

La notificación de actualización de Management Server activa el proceso de colocación en la antememoria a fin de actualizar todas las réplicas. Estas notificaciones de actualización tienen lugar siempre que se producen cambios en la base de datos primaria de políticas de autorización.



Notas sobre el rendimiento:

- Management Server envía directamente notificaciones de actualización a los servidores de aplicaciones. Los servidores de aplicaciones comprueban la versión de la base de datos primaria de políticas de autorización cada pocos minutos. Con esta comprobación se asegura que los servidores de aplicaciones no hayan olvidado una notificación de actualización.

  Si una notificación de actualización no llega correctamente a un servidor, Policy Director crea una entrada en las anotaciones cronológicas. En ambos casos, un mecanismo de repetición se asegura de que la actualización se realice posteriormente.
- La colocación en la antememoria de la información sobre políticas de autorización consigue un alto rendimiento del sistema. Por ejemplo, cuando WebSEAL efectúa una comprobación de autorización, comprueba la plantilla de la política en su propia versión de la base de datos situada en la antememoria. WebSEAL no tiene que acceder a la red para obtener la información de la base de datos primaria. El resultado son tiempos de respuesta (rendimiento) cortos en las comprobaciones de autorizaciones.
- El servidor de aplicaciones de llamada no coloca en la antememoria los resultados de autorizaciones individuales.

Política de seguridad de la red

La forma de controlar la participación de usuarios y de grupos en el dominio determina la política de seguridad de un dominio seguro. La política de seguridad aplica normas a los recursos que requieren protección. Estas normas se conocen como *plantillas de políticas.*

Policy Director Authorization Service aplica la política comparando la identidad y las credenciales de un usuario con la plantilla de política asignada al recurso solicitado. Policy Director pasa la recomendación al gestor de recursos, que completa la respuesta a la petición original.

Definición de política de seguridad de la red

Policy Director Authorization Service utiliza una base de datos central que lista todos los recursos del dominio seguro y las plantillas de políticas asignadas a cada

recurso. Esta base de datos primaria de políticas de autorización y el registro de seguridad son los componentes clave que ayudan a definir la política de seguridad de una red. El registro de seguridad contiene cuentas de usuarios y de grupos.

Resumiendo, una política de seguridad de red controla:

- Usuarios y grupos autorizados a participar en el dominio seguro. El registro de seguridad contiene y mantiene esta información.
- El nivel de protección sobre todos los objetos del dominio seguro.La base de datos primaria de políticas de autorización mantiene esta información.

Espacio de nombres de objetos protegidos

El *espacio de nombres de objetos protegidos* es una descripción jerárquica de los recursos que pertenecen a un dominio seguro. Los objetos que aparecen en el espacio de nombres jerárquico representan los recursos reales de la red.

- **Recurso del sistema** — el archivo físico, servicio de red o aplicación reales.
- **Objeto protegido** — la representación lógica de un recurso real del sistema utilizado por Policy Director Authorization Service, Management Console y demás programas de utilidad de Policy Director.

Para proporcionar seguridad a un recurso pueden unirse plantillas de políticas a objetos del espacio de nombres. Policy Director Authorization Service toma decisiones sobre autorizaciones basándose en esas plantillas.

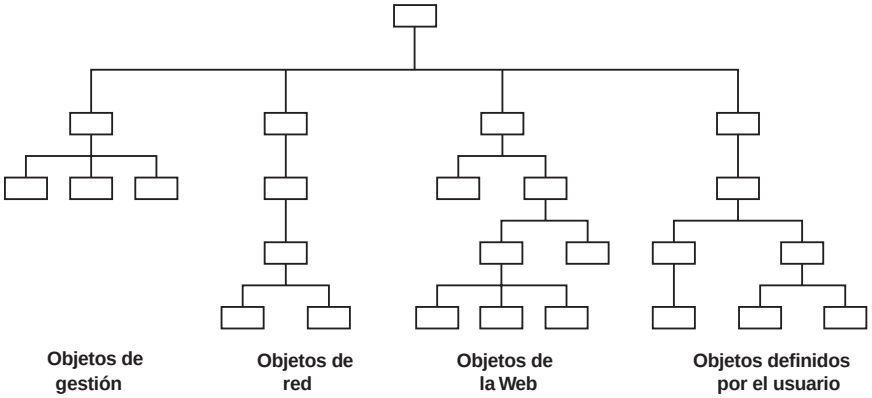
Policy Director utiliza las siguientes categorías de espacios de nombres:

Objetos de la Web
Estos objetos representan cualquier cosa que un URL de HTTP pueda direccionar, como páginas Web estáticas y URL dinámicos. Puede convertir las páginas Web estáticas y los URL dinámicos en consultas a la base de datos o en algún otro tipo de aplicación.

Objetos de la red
Estos objetos representan aplicaciones basadas en TCP (como TELNET y FTP) que se correlacionan las con direcciones de la red TCP (puertas) que están utilizando las aplicaciones.

Objetos de gestión
Estos objetos representan las actividades de gestión que pueden realizarse utilizando Policy Director Management Console. Los objetos representan las tareas necesarias para definir usuarios y establecer políticas de seguridad. Policy Director permite la delegación de actividades de gestión y puede restringir la posibilidad de un administrador de establecer políticas de seguridad a un subconjunto del espacio de nombres.

Objetos definidos por el usuario
Estos objetos representan tareas o recursos de la red protegidos por aplicaciones de terceros que utilicen Policy Director Authorization Service, que a su vez utiliza la API de autorizaciones de Policy Director.



Definición y aplicación de plantillas de políticas

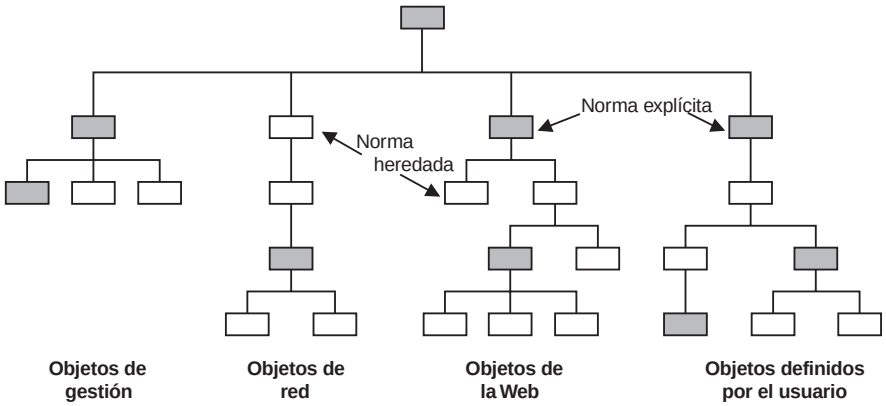
Los administradores de seguridad protegen los recursos del sistema definiendo normas (plantillas de políticas) y aplicándolas a las representaciones de objetos de dichos recursos en el espacio de nombres.

Policy Director Authorization Service toma decisiones sobre autorizaciones basándose en las plantillas de políticas que se aplican a esos objetos. Cuando Policy Director permite la ejecución de una operación solicitada sobre un objeto protegido, la aplicación responsable del recurso lleva a cabo la operación.

Una plantilla de política puede indicar los parámetros de protección de muchos objetos. Cualquier modificación en la norma afectará a todos los objetos a los que se refiera la norma.

Política explícita y heredada

Una política puede heredarse o aplicarse explícitamente. El espacio de nombres de objetos protegidos de Policy Director permite heredar atributos de la política de seguridad. Este es un punto importante que debe tener en cuenta el administrador de seguridad que gestiona el espacio de nombres. El administrador sólo tendrá que aplicar plantillas de políticas explícitas en los puntos de la jerarquía en los que las normas deben cambiar.



Entre las plantillas de políticas se incluyen:

- Normas codificadas originalmente
- Posibilidad de autorización externa
- Etiquetas de seguridad especiales

- Listas de control de acceso

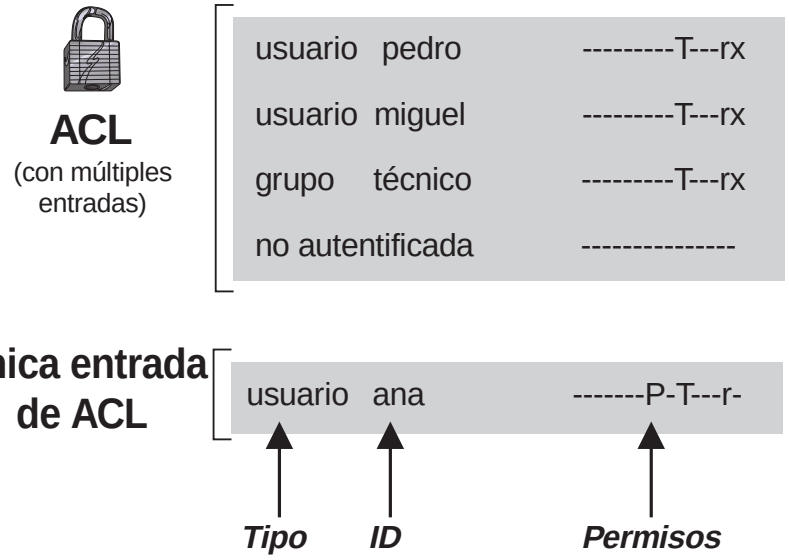
Lista de control de accesos

Por ejemplo, una lista de control de accesos (ACL) es una plantilla de política. Policy Director utiliza ACL como plantilla de política primaria.

Una ACL es un conjunto de controles (permisos) que especifica las condiciones necesarias para llevar a cabo determinadas operaciones en un recurso. Las definiciones de las ACL son componentes importantes de la política de seguridad que se establece para el dominio seguro. Las ACL, como todas las plantillas de políticas, se utilizan para estampar un sello con la política de seguridad de una empresa en los recursos representados en el espacio de nombres de objetos protegidos.

Una ACL controla específicamente:
- Las operaciones realizadas en el recurso.
- Las personas que pueden realizar dichas operaciones.

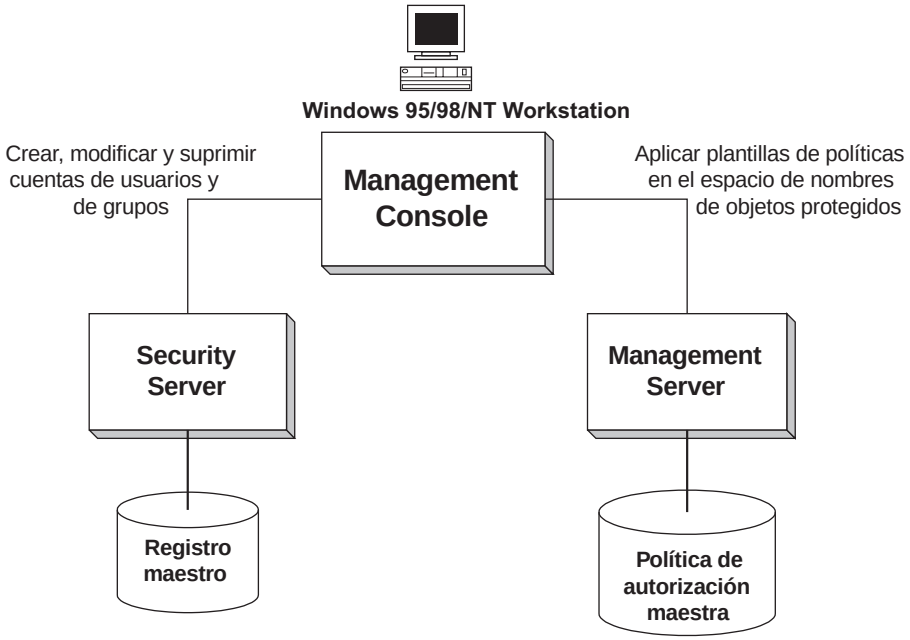
Una ACL está formada por una o más entradas, incluidas las designaciones de usuarios y de grupos más sus permisos o derechos específicos.



Administración de políticas

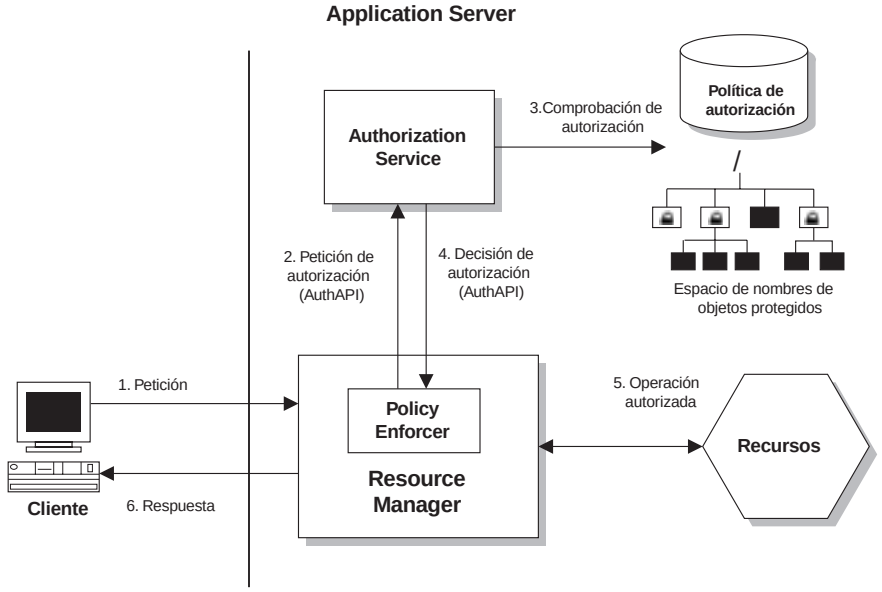
Policy Director Management Console es una aplicación gráfica basada en Java que se utiliza para gestionar la política de seguridad de un dominio seguro de Policy Director. El programa de utilidad de línea de mandatos **ivadmin** opcional tiene las mismas posibilidades administrativas que Management Console.

Desde Management Console o utilizando el programa de utilidad **ivadmin** podrá gestionar el registro de Security Server, la base de datos primaria de políticas de autorización y todos los servidores de Policy Director. También podrá añadir o suprimir usuarios y grupos y aplicar plantillas de políticas o ACL a objetos de la red.



Proceso de autorización paso a paso

El siguiente diagrama ilustra el proceso completo de autorización:



1. Policy Director dirige al servidor del gestor de recursos una petición de un cliente autentificado para un recurso. El proceso del aplicador de política intercepta la petición.

   El gestor de recursos puede ser WebSEAL (para acceso HTTP y HTTPS), NetSEAL (para acceso TCP/IP de red) o una aplicación de terceros.

2. El proceso aplicador de política utiliza la API de autorizaciones (consulte el apartado “API de autorizaciones de Policy Director” en la página 48) para llamar a Policy Director Authorization Service para que tome una decisión sobre una autorización.

3. El servicio de autorizaciones efectúa una comprobación de autorización sobre el recurso que aparece representado como un objeto en el espacio de nombres de objetos protegidos de Policy Director. La plantilla de política aplicada al objeto se comprueba con las credenciales del cliente.
4. Se devuelve al gestor de recursos una recomendación (utilizando el aplicador de política) para aceptar o denegar la petición.
5. Si la comprobación de autorización aprueba la petición, el gestor de recursos pasará la petición a la aplicación responsable del recurso.
6. El cliente recibirá los resultados de la operación solicitada.

API de autorizaciones de Policy Director

La *interfaz de programas de aplicación* (API) de Policy Director Authorization permite a aplicaciones de Policy Director y de terceros solicitar a Policy Director Authorization Service que tome decisiones sobre autorizaciones.

La API de autorizaciones de Policy Director es la interfaz entre el gestor de recursos (que solicita la comprobación de autorización) y el servicio de autorizaciones propiamente dicho. La API de autorizaciones de Policy Director permite que la aplicación que hace cumplir la política solicite una decisión sobre una autorización. Sin embargo, la API de autorizaciones de Policy Director evita a la aplicación las complejidades del proceso real de toma de decisiones.

La API de autorizaciones de Policy Director facilita un modelo de programación estándar para codificar las peticiones de autorizaciones y las decisiones sobre las mismas. La API de autorizaciones de Policy Director permite efectuar llamadas estandarizadas al servicio de autorizaciones gestionado centralmente desde cualquier aplicación antigua o recién desarrollada.

La API de autorizaciones de Policy Director puede utilizarse de una de dos formas:

Modalidad de antememoria remota
En esta modalidad, Policy Director inicializa la API para que llame a Policy Director Authorization Server (ivacld) a fin de que tome decisiones sobre autorizaciones en nombre de la aplicación. Policy Director Authorization Server mantiene su propia antememoria de la réplica base de datos de políticas de autorización. Utilice esta modalidad para gestionar las peticiones de autorización de clientes de la aplicación.

Consulte el apartado “Modalidad de antememoria remota” en la página 50.

Modalidad de antememoria local
En esta modalidad, Policy Director inicializa la API para bajar y mantener una réplica local de la base de datos de autorizaciones para la aplicación. La modalidad de antememoria local permite a la aplicación tomar localmente todas las decisiones de autorización, consiguiendo de este modo un mejor rendimiento y fiabilidad.

Sin embargo, debido a la actividad general que representa la reproducción de la base de datos y a las implicaciones que tiene sobre la seguridad la utilización de esta modalidad aconsejan su empleo para servidores de aplicaciones fiables. Entre los servidores de aplicaciones fiables se encuentran WebSEAL y NetSEAL.

Consulte el apartado “Modalidad de antememoria local” en la página 51.

La posibilidad de evitar al usuario las complejidades del mecanismo del servicio de autorizaciones propiamente dicho es una de las cualidades de la API de

autorizaciones de Policy Director que proporciona muchas ventajas. Tras la API de autorizaciones de Policy Director, Policy Director oculta los problemas que representan la gestión, el almacenamiento, la colocación en la antememoria, la reproducción, los formatos de credenciales y los métodos de autentificación .

La API de autorizaciones de Policy Director también funciona independientemente de la infraestructura de seguridad subyacente, el formato de credenciales y el mecanismo de evaluación. La API de autorizaciones de Policy Director permite solicitar una comprobación de autorización y obtener la devolución de una simple recomendación “sí” o “no” como respuesta. Los detalles del mecanismo de autorización son invisibles para el usuario.

La API de autorizaciones de Policy Director proporciona soporte para las siguientes plataformas:

- Microsoft Windows NT, Windows 98 y Windows 95
- IBM AIX Versión 4.3
- Sun Solaris Versión 2.6

Ejemplos de la API de autorizaciones

Los servicios de autorizaciones de WebSEAL y NetSEAL realizan el control de accesos en URL y puertas respectivamente. Una aplicación de terceros puede utilizar la API de autorizaciones de Policy Director para efectuar el control de accesos en procesos extremadamente específicos y especializados.

Ejemplo 1: Se puede diseñar una interfaz gráfica de usuario (GUI) para mostrar dinámicamente los botones de tareas como activos o inactivos, según sean los resultados de la comprobación de autorización.

Ejemplo 2: Las siguientes figuras muestran otra utilización de la API de autorizaciones de Policy Director. Esta figura muestra una petición de una transacción CGI hecha por una aplicación de la Web.

El nivel inferior de autorización, ilustrado en la Figura A, implica un control de accesos de “todo o nada” al URL. Este nivel flexible de autorización sólo determina si el cliente puede ejecutar el programa CGI. Al permitir el acceso a la aplicación CGI, ningún otro control estará disponible para los recursos manipulados por la aplicación CGI.

En la Figura B, los controles de acceso son un conjunto de recursos manipulados por el programa CGI. La aplicación de la Web se ha configurado para que utilice la API de autorizaciones de Policy Director. Ahora, el programa CGI puede llamar al Policy Director Authorization Service para tomar decisiones de autorización sobre los recursos que manipula. Las decisiones de autorización pueden basarse en la identidad del cliente que efectúa la petición.

Figura A

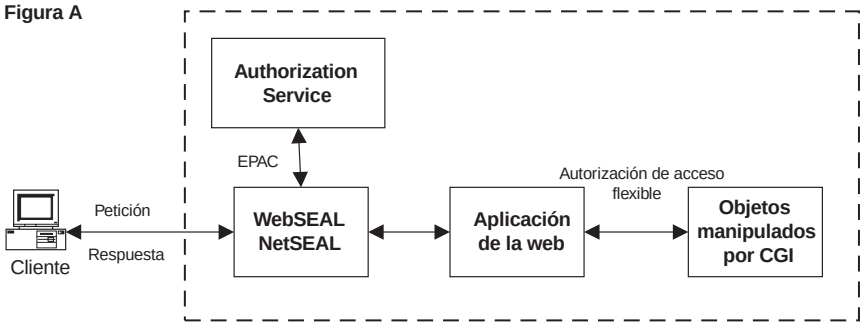
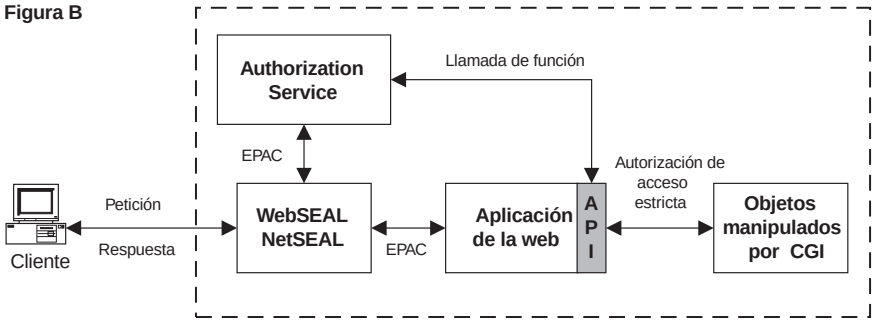


Figura B

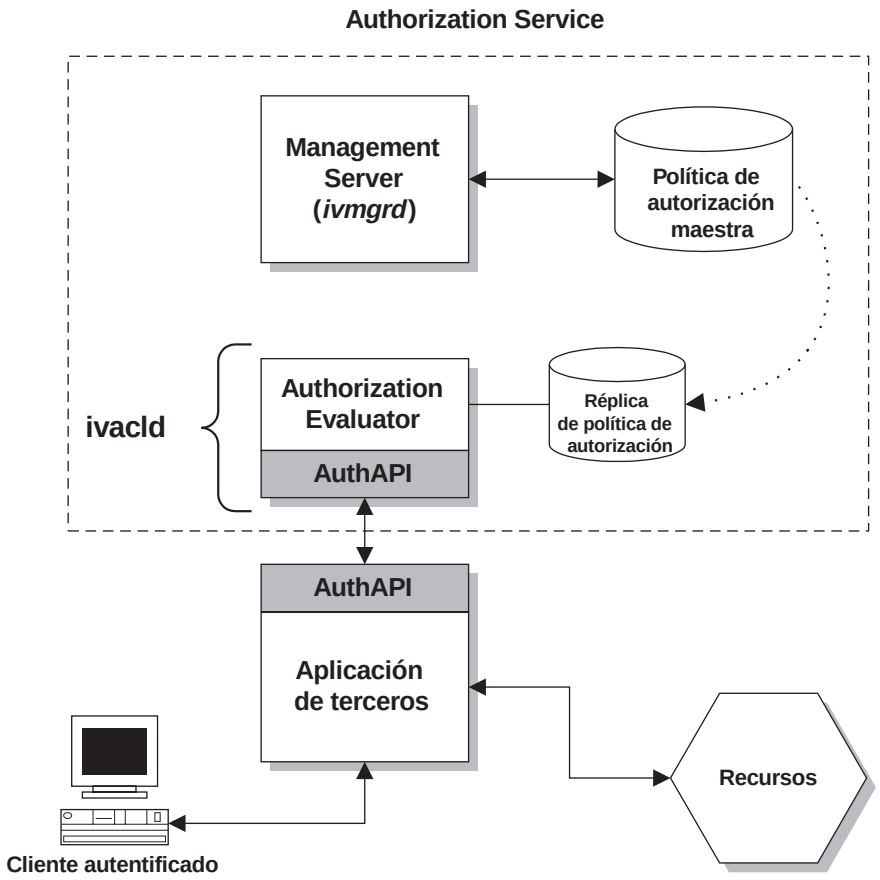


Modalidad de antememoria remota

En *modalidad de antememoria remota*, las aplicaciones utilizan las llamadas de función proporcionadas por la API de autorizaciones de Policy Director para comunicarse con Policy Director Authorization Server (ivacld) remoto. Policy Director Authorization Server funciona como evaluador de toma de decisiones de autorización y mantiene su propia réplica de la base de datos de políticas de autorización.

Policy Director Authorization Server toma la decisión y devuelve una recomendación a la aplicación utilizando la API. El servidor también puede grabar un registro de auditoría que contenga los detalles de la petición de decisión de autorización.

Debe haber un Policy Director Authorization Server funcionando en algún lugar del dominio seguro. Policy Director Authorization Server puede residir en la misma máquina que la aplicación o en otra máquina. Policy Director Authorization Server también puede instalarse en más de una máquina de un dominio seguro para que la disponibilidad sea más alta. La API de autorizaciones de Policy Director da un error de forma transparente cuando un Policy Director Authorization Server determinado no se ejecuta correctamente.



Modalidad de antememoria local

En *modalidad de antememoria local*, la API baja y mantiene una réplica de la base de datos de políticas de autorización en el sistema de archivos local de la aplicación. Toma todas las decisiones de autorización en la memoria consiguiendo de este modo un mejor rendimiento y una mayor fiabilidad.

La réplica local sigue existiendo después de las llamadas de la aplicación. La API se inicia en modalidad de réplica. Cuando se inicia, comprueba si hay alguna actualización en la base de datos primaria de políticas de autorización. Son las actualizaciones que pueden haberse producido desde la creación de la réplica local.

Figura A

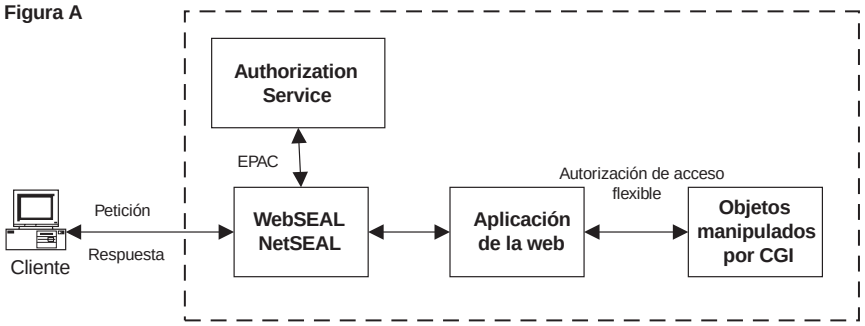
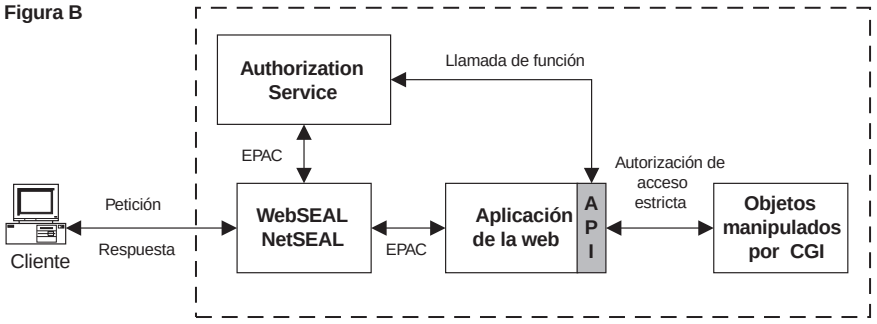


Figura B



Posibilidad de autorización externa

En algunas situaciones, es posible que el conjunto estándar de permisos de Policy Director no pueda expresar todas las normas de autorización que requiera una de las políticas de seguridad de una empresa. Policy Director utilizará entonces la posibilidad opcional de autorización externa para obtener todos los requisitos de autorización suplementarios que sean necesarios.

Un servicio de autorizaciones externo permite imponer condiciones y controles de autorización adicionales indicados por un programa servidor de autorizaciones externo y distinto.

Ampliación del servicio de autorizaciones

Policy Director Authorization Service incorpora automáticamente un servicio de autorizaciones externo. Si se configura un servicio de autorizaciones externo, Policy Director Authorization Service simplemente incorporará los nuevos controles y condiciones a su proceso de evaluación.

Las aplicaciones que utilizan Policy Director Authorization Service incluyen WebSEAL, NetSEAL y cualquier aplicación que utilice la API de autorizaciones de Policy Director. Estas aplicaciones aprovechan la contribución adicional y sin problemas de un servicio de autorizaciones configurado externo. Las adiciones efectuadas a la política de seguridad mediante la utilización de un servicio de autorizaciones externo son transparentes para dichas aplicaciones y no requieren ningún cambio en las mismas.

La arquitectura del servicio de autorizaciones externo permite la integración completa del servicio de seguridad ya existente en una empresa. Un servicio de autorizaciones externo conserva la inversión inicial de la empresa en mecanismos

de seguridad. Estos servicios de autorizaciones externos permiten la incorporación de los servidores heredados en el proceso de toma de decisiones de autorización de Policy Director.

La puesta a punto de un servicio de autorizaciones externo requiere la realización de estas dos operaciones generales:

1. Escribir un programa servidor al que se hará referencia durante la toma de decisión de una autorización.
2. Registrar el servicio de autorizaciones externo con Policy Director.

Después de registrar el servicio, un nuevo permiso que representará al servicio aparecerá en la consola de Policy Director Management Console. A partir de ese momento, podrá utilizar ese permiso en cualquier entrada de la ACL.

Cuando se encuentre ese permiso durante la comprobación de la autorización, se consultará al servicio de autorizaciones externo para tomar decisiones adicionales de autorización.

Encontrará información detallada sobre la configuración del servicio de autorizaciones externo en el manual *Policy Director Programmer's Guide and Reference*.

Condiciones en peticiones de recursos

Un servicio de autorizaciones externo también puede utilizarse para imponer una condición específica para que un intento de acceso sea o no aceptado.

Estas condiciones pueden ser, entre otras:

- Hacer que un mecanismo de auditoría externo registre si el intento de acceso ha sido o no aceptado.
- Supervisar activamente el intento de acceso e incorporar una alerta o alarma cuando se detecte un comportamiento inaceptable.
- Transacciones de facturación y de micropagos.

Proceso de evaluación de autorizaciones

Una decisión de autorización que incorpore un servicio de autorizaciones externo se produce como sigue:

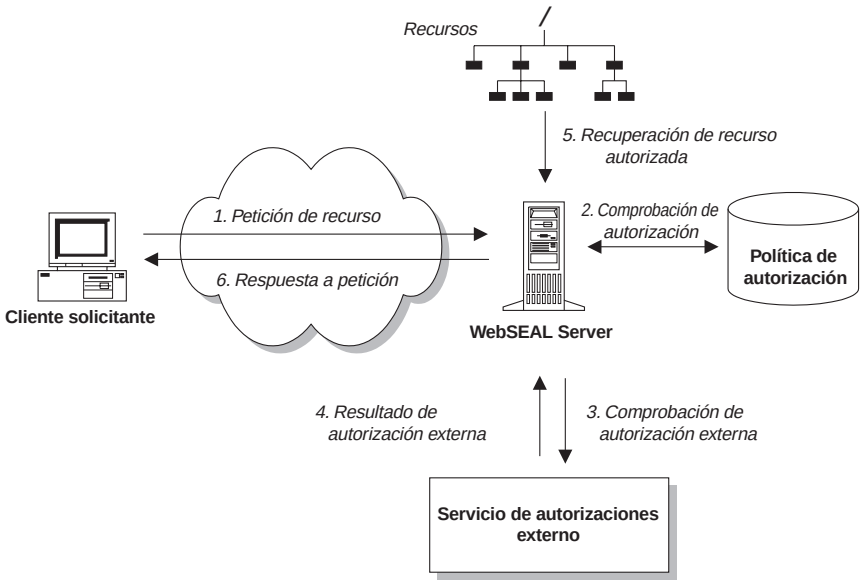
1. Se efectúa una comprobación de ACL para determinar el conjunto de permisos otorgado al usuario que efectúa la solicitud.
2. Se envía una petición de autorización que utilice RPC a cada servicio de autorizaciones externo cuyo permiso aparezca en la ACL.

   Esta comprobación de autorización externa se produce independientemente de si la autorización necesaria se otorga o no al usuario.
3. Se suman todos los resultados de las decisiones de autorización.

   Las denegaciones pueden proceder de la comprobación de la ACL de Policy Director o de la comprobación de cualquier servicio de autorizaciones externo. Si se produce alguna denegación, Policy Director Authorization Service rechazará la petición de autorización.

Ejemplo:

La siguiente figura ilustra una decisión de autorización que implica a un WebSEAL Server y a un servicio de autorizaciones externo.



En este ejemplo, la finalidad del servicio de autorizaciones externo es imponer limitaciones de tiempo en el acceso a objetos. El carácter asignado para representar el permiso en Management Console es la k.

1. Policy Director WebSEAL Server recibe una petición de un cliente que desea acceder a un documento técnico confidencial. El cliente es miembro del grupo técnico.
2. Primero, WebSEAL Server comprueba la réplica de la base de datos de políticas de autorización para determinar los permisos asignados al objeto de documento.

   ```
   grupo técnico rk
   ```

   Si la entrada de la ACL no contiene el permiso del servicio de autorizaciones externo, la decisión final en cuanto a la autorización se basará únicamente en esta información.

   En el ejemplo de arriba, la entrada de la ACL contiene un permiso de lectura estándar. La entrada también contiene un permiso (k) adicional que hace referencia a un servidor de autorizaciones externo que suplementa la evaluación de la autorización.
3. Policy Director utiliza una RPC autentificada al servidor de autorizaciones externo a fin de enviar una petición. El conjunto de permisos otorgados se determina en el paso 2. Policy Director envía este conjunto de permisos con esta petición para que el servidor de autorizaciones externo pueda basar su decisión en dicha información.

   En este ejemplo, el diseño del servidor de autorizaciones externo permite definir límites de tiempo en la posibilidad de acceso al documento. El acceso al documento sólo se lleva a cabo cuando la petición se produce entre las 8 de la mañana y las 6 de la tarde, de lunes a viernes.
4. El cliente de este ejemplo efectúa la petición a las 10 de la mañana de un martes. El servidor devuelve una respuesta afirmativa al WebSEAL Server.

   La suma total de todas las decisiones de autorización anteriores tiene como resultado una recomendación final de permitir el acceso al objeto de documento.
5. WebSEAL Server recupera el recurso de documento.

6. WebSEAL Server permite al cliente ver el documento.

En el manual *Policy Director Programmer's Guide and Reference* encontrará información detallada para la activación del servicio de autorizaciones externo.

Estrategias de implementación

Policy Director permite la utilización de un servicio de autorizaciones externo de varias formas:

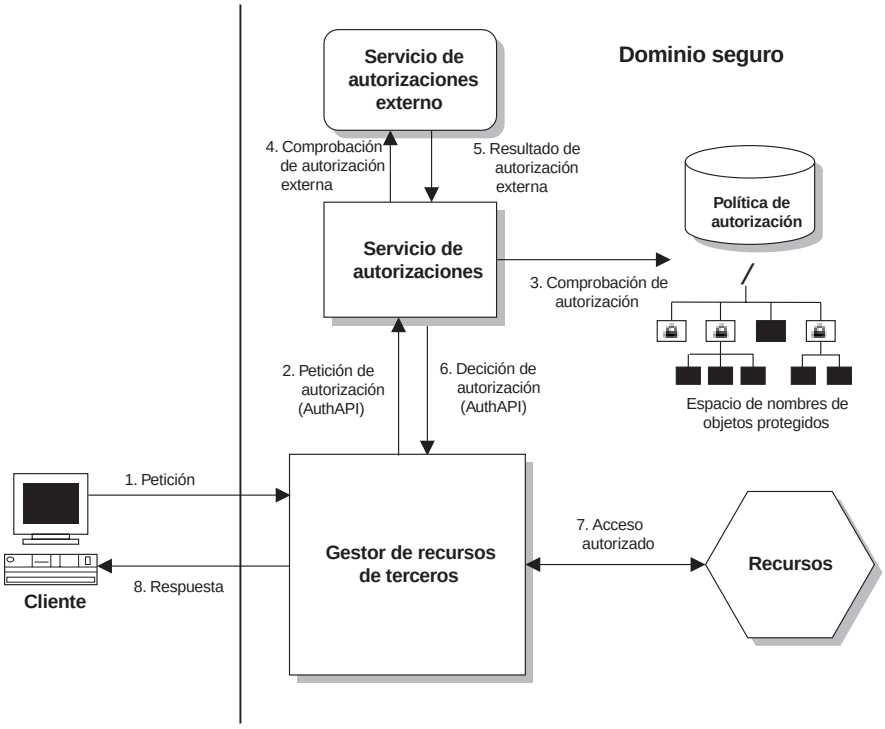
- Se pueden añadir al dominio seguro tantos servicios de autorizaciones externos como se desee para que desempeñen distintas evaluaciones de autorización. En una ACL, cada permiso distinto representa un servicio.
- Para un permiso determinado, se puede llamar a más de un servidor externo encadenando varios servidores de autorizaciones externos. Cada uno de ellos pasará la identidad autentificada al siguiente servidor de la cadena y recogerá los resultados de toda la corriente de servidores.
- Un servicio de autorizaciones externo puede reproducirse a lo largo de todo el dominio seguro.

Cada una de estas implementaciones es independiente de la otra y puede utilizarse en cualquier combinación.

Posibilidad de ampliación y flexibilidad

La combinación de la API de autorizaciones de Policy Director y de un servicio de autorizaciones externo proporciona una solución altamente ampliable y flexible para ejecutar una política de seguridad.

La siguiente figura ilustra la arquitectura ampliable posible utilizando las características combinadas de la API de autorizaciones para una aplicación de terceros y un servicio de autorizaciones externo:



Capítulo 4. Presentación de Management Console

Policy Director Management Console es una aplicación gráfica basada en Java que se utiliza en una red distribuida para gestionar con seguridad todos los componentes de Policy Director. Desde Management Console podrá gestionar el registro de Security Server, la base de datos primaria de políticas de autorización y todos los servidores de Policy Director. Management Console también permite añadir y suprimir usuarios o grupos y aplicar distintas ACL.

Este capítulo incluye los siguientes temas:

Visión general de Management Console

Policy Director Management Console es una aplicación gráfica basada en Java que se utiliza para gestionar la política de seguridad de un dominio seguro de Policy Director. El programa de utilidad de línea de mandatos **ivadmin** opcional tiene las mismas posibilidades administrativas que Management Console.

Desde Management Console o mediante el programa de utilidad **ivadmin** tendrá la posibilidad de:

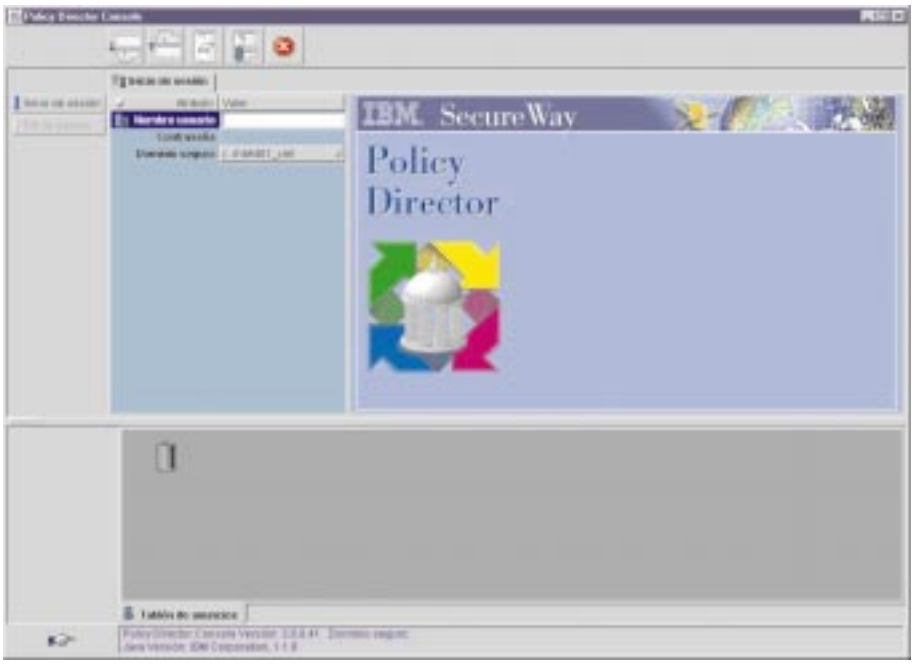
- Modificar la base de datos de registros (cuentas).
- Modificar la base de datos de políticas de autorización (ACL).
- Añadir y suprimir usuarios.
- Añadir y suprimir grupos.
- Aplicar plantillas de políticas o ACL a objetos.
- Añadir, suprimir o modificar recursos Global Sign-on (GSO), grupos de recursos y credenciales de recursos.
- Añadir, eliminar o cambiar un usuario proxy (opcional)

Características de Management Console

Management Console proporciona herramientas para realizar tareas y visualiza información en distintas áreas de la ventana de Management Console. Las áreas de pantalla y herramientas primarias incluyen:

- Separadores de tareas
- Paneles de tareas de gestión (paneles superiores e inferiores)
- Botones de acción
- Barra de herramientas
- Tablón de anuncios (panel inferior por omisión)

- Barra de estado
- Barra de títulos



Herramientas del panel de tareas de gestión

Estas herramientas se proporcionan para los paneles de tareas de gestión:

- Separadores de tareas
- Paneles de tareas de gestión (paneles superiores e inferiores)
- Botones de acción

Separadores de tareas

Management Console proporciona estos *separadores de tareas* para ejecutar operaciones de gestión:

- Inicio de sesión
- Usuarios
- Grupos
- Recursos GSO
- Grupos de recursos GSO
- ACL
- Espacio de objetos
- Usuario proxy (opcional)

Paneles de tareas de gestión

Cada separador de tareas produce un panel de tarea de gestión que incluye un grupo de vistas de información presentadas en el panel superior de Management Console.

Las tareas de gestión incluyen:

Inicio de sesión El inicio de sesión es el punto de entrada para el inicio y fin de sesión con Management Console.

Usuarios	Permite crear y mantener usuarios que participen del dominio seguro.
Grupos	Permite crear y mantener grupos en el dominio seguro.
Recursos GSO	Permite crear y mantener información sobre recursos GSO.
Grupos de Recursos GSO	Permite crear y mantener información sobre grupos de recursos GSO.
ACL	Permite crear y mantener plantillas de políticas o ACL.
Espacio de objetos	Permite unir plantillas de políticas a objetos en el espacio de nombres así como suprimir dichas plantillas de los objetos del espacio de nombres.
Usuario Proxy	Permite crear y mantener información sobre un usuario proxy.

Botones de acción

Cada separador de tareas dispone de un conjunto específico de botones de acción. Utilice estos botones de acción para efectuar operaciones de administración. Los botones aparecen en el lado izquierdo del panel. Los botones de acción cambian y actualizan la base de datos correspondiente.

Tipos de vistas de paneles

La información de los paneles de tareas de gestión puede visualizarse de una de estas tres formas. Cada tipo de vista tiene características específicas.

Vista de detalles

Una vista de detalles contiene campos dinámicos para la entrada de datos.

Vista de lista

Una vista de lista puede clasificarse en orden ascendente o descendente pulsando el botón en la barra de títulos de la columna adecuada. En algunas de las listas pueden efectuarse consultas.

Vista de árbol

Una vista de árbol puede ampliarse y reducirse.

Cuando se selecciona un elemento que está activo en alguna de las vistas, el resaltado aparece en azul.

Cuando se selecciona un elemento que no está activo en ese momento se utiliza el color gris.

Barra de herramientas

La barra de herramientas aparece en la parte superior de la ventana de Management Console y contiene botones que activan funciones específicas de Management Console.

El botón **Colocar tarea abajo** vuelve a colocar la tarea de gestión actual del panel superior en el panel inferior.

El botón **Colocar tarea arriba** vuelve a colocar la tarea de gestión actual del panel inferior en el panel superior.

El botón **Vista de chincheta** toma la información que está activa en ese momento en el panel superior y coloca una copia de dicha información en el panel inferior. La información activa en el panel superior contiene información como, por ejemplo, una lista de grupos o de usuarios. También aparece un nuevo separador correspondiente al panel. La información de este panel es únicamente una copia estática que no es dinámica. Sin embargo, podrá seguir ampliando y reduciendo las vistas de árbol como, por ejemplo, el árbol del espacio de objetos y la lista de grupos.

El botón **Borrar** borra de Management Console la vista seleccionada en ese momento. Esta acción borra únicamente la vista y ello no afecta a la información real de la base de datos.

El botón **Detener** interrumpe la acción que está realizándose en ese momento y devuelve el control de Management Console al administrador. En realidad, ignora el resultado de la acción en curso y Management Console se comporta como si la operación no se hubiese efectuado correctamente.

Tablón de anuncios

Tablón de anuncios es el panel inferior por omisión de Management Console. El tablón de anuncios se utiliza como ubicación temporal de almacenamiento de cualquier objeto que se desee utilizar varias veces durante una sesión de administración. Entre los objetos puede haber archivos, listas de usuarios y de grupos, y atributos. Los iconos de objetos se arrastran y se sueltan en el tablón de anuncios y se utilizan en las tareas de administración cuando se necesitan.

Los iconos estándar del tablón de anuncios son el icono de **Papelera** y el icono de **Vista de chincheta**.

Icono de Papelera

Los iconos que se encuentran en el tablón de anuncios pueden eliminarse arrastrándolos hasta el icono de **Papelera**.

Panel de Vista de chincheta

Puede seleccionar (resaltar) objetos e información específicos desde cualquiera de los paneles de tareas de gestión y arrastrarlos hasta el icono de **Vista de chincheta** del Tablón de anuncios.

Esta acción produce un nuevo panel inferior que visualiza una copia de la información seleccionada. También aparece un nuevo separador .

La información de este panel es únicamente una copia estática que no es dinámica. Sin embargo, podrá seguir ampliando y reduciendo las vistas de árbol como, por ejemplo, el árbol del espacio de objetos y la lista de grupos.

Si la información activa es una lista de grupos, en el panel de la vista de chincheta sólo se colocarán los grupos seleccionados (resaltados).

Para cerrar un panel de Vista de chincheta, pulse el botón de cierre del cuadro que se encuentra en el ángulo superior derecho de la ventana de Microsoft Windows.

Nota: Lo mismo se produce cuando se selecciona la información y se pulsa el botón **Vista de chincheta** en la barra de herramientas.

Barra de estado

La barra de estado de la parte inferior de Management Console visualiza mensajes de estado y de error.

- La información sobre el estado general aparece en **negro**.
- Los avisos aparecen en **azul**.
- Los errores aparecen en **rojo**.

A la izquierda del área de mensajes aparece un icono indicador de estado:


icono de Estado correcto


Icono de estado de aviso


Icono de estado erróneo

Si efectúa una doble pulsación en el icono de indicador de estado, la barra de estado visualizará:

- La versión de Management Console
- El dominio seguro afectado por la actividad de Management Console
- La versión de Java

Barra de título

La barra de título de Management Console visualiza dos partes importantes de la información:

- El dominio seguro en que se efectúa en ese momento la actividad de Management Console.
- El estado de la sesión iniciada por el usuario (UPDATE o READ-ONLY) (ACTUALIZACIÓN o SÓLO LECTURA).

Si el registro del Security Server no está disponible, no podrá efectuar modificaciones en los datos de contabilidad a través de Management Console. En esta situación poco frecuente, Management Console obtiene la información actual de cuentas de réplicas del registro. Si intenta cambiar la información que afecta al registro, aparecerá un mensaje de error.

Tarea de gestión de inicio de sesión

El panel de la tarea de inicio de sesión es el punto de entrada a Management Console para un usuario autentificado. Si esta acción se efectúa correctamente, aparecerá el conjunto completo de separadores de tareas de gestión.

Cuando el usuario finaliza la sesión, todo el contexto se pierde y los separadores desaparecen.

Separador de tarea

Separador de tarea: **Inicio de sesión**

Tarea de gestión

El panel de la tarea de gestión de inicio de sesión contiene campos para las entradas de **Nombre de usuario** y de **Contraseña**. El campo **Dominio seguro** visualiza inicialmente el dominio seguro por omisión configurado para NetSEAT.

El menú Inicio de sesión permite seleccionar distintos dominios seguros para realizar en ellos tareas de Management Console.

Botones de acción

Los botones de acción de **Inicio de sesión** son:

- Inicio de sesión
- Fin de sesión

Tarea de gestión de usuarios

El panel de la tarea de gestión Usuarios permite crear y mantener usuarios que participen del dominio seguro. Cuando se selecciona un usuario de la vista de lista o de la vista de árbol, los campos de la vista de detalles se rellenan con los datos actuales.

Separador de tarea

Separador de tarea: **Usuarios**

Tarea de gestión

El panel de tarea de gestión Usuarios contiene una vista de lista de Usuarios, una vista Detalle de usuario y una vista de lista Grupos.

La vista Grupos contiene otros separadores para Recursos GSO y Grupos de Recursos GSO.

Botones de acción

Los botones de acción de **Usuarios** son:

- Nuevo
- Obtener
- Guardar
- Eliminar

Tarea de gestión de grupos

El panel de la tarea de gestión Grupos permite crear y mantener grupos en el dominio seguro. Cuando se selecciona un grupo de la vista de lista o de la vista de árbol, los campos de la vista de detalles se rellenan con los datos actuales.

Separador de tarea

Separador de tarea: **Grupos**

Tarea de gestión

El panel de la tarea de gestión Grupos contiene una vista de lista Grupos, una vista de Detalle de Grupo y una vista de lista ID de usuario.

Botones de acción

Los botones de acción de **Grupos** son:

- Nuevo
- Obtener
- Guardar
- Eliminar

Tarea de gestión de recursos GSO

El panel de tarea de gestión Recursos GSO permite crear y mantener Recursos GSO en el dominio seguro. Los recursos GSO son siempre recursos de la Web. Cuando se selecciona un recurso GSO de la vista de lista o de la vista de árbol, los campos de la vista de detalles se rellenan con los datos actuales.

Separador de tarea

Separador de tarea: **Recursos GSO**

Tarea de gestión

El panel de tarea de gestión Recursos GSO contiene una vista de lista Recursos y una vista de detalles de recursos.

Botones de acción

Los botones de acción de **Recursos GSO** son:

- Nuevo
- Obtener
- Guardar

- Eliminar

Tarea de gestión de grupos de recursos GSO

El panel de tarea de gestión Grupos de recursos GSO permite crear y mantener grupos de recursos GSO en el dominio seguro. Un *grupo de recursos* indica un grupo de servidores de la Web en el que todos los servidores del grupo tienen el mismo conjunto de ID de usuario y la misma contraseña. Cuando se selecciona un grupo de recursos GSO de la vista de lista o de la vista de árbol, los campos de la vista de detalles se rellena con los datos actuales.

Se puede crear una sola credencial de recurso para todos los recursos del grupo de recursos. Policy Director utiliza una sola credencial de recurso para un grupo de recursos en vez de crear una credencial de recurso para cada recurso del grupo de recursos.

Separador de tarea

Separador de tarea: **Grupos de Recursos GSO**

Tarea de gestión

El panel de la tarea de gestión Grupo de recursos GSO contiene una vista de lista Grupos de recursos, una vista Detalle de grupo de recursos y una vista de lista Recursos GSO.

Botones de acción

Los botones de acción de **Grupos de recursos GSO** son:

- Nuevo
- Obtener
- Guardar
- Eliminar

Tarea de gestión de ACL

El panel de tarea de gestión ACL permite crear y mantener plantillas de políticas ACL. Cuando se selecciona una ACL de la vista **Lista de ACL**, los campos de la vista Definición de ACL se rellenan con los datos actuales.

Separador de tarea

Separador de tarea: **ACL**

Tarea de gestión

El panel de la tarea de gestión ACL contiene una vista Lista de ACL, una vista de detalles Definición de ACL y una vista de detalles Entrada de ACL con una vista de árbol de los permisos.

Botones de acción

Los botones de acción de **ACL** son:

- Nueva ACL
- Nueva entrada
- Guardar
- Eliminar

- Obtener
- Listar
- Dónde se usa

Tarea de gestión de espacio de objetos

El panel de la tarea de gestión Espacio de objetos permite unir listas de ACL a objetos del espacio de nombres así como eliminarlas de dichos objetos del espacio de nombres.

Cuando se selecciona un objeto en la vista de árbol Espacio de objetos, la secuencia de ACL heredadas aparece en la vista de árbol ACL heredadas. Esta lista indica todos los objetos que tienen definidas explícitamente ACL que afectan a los permisos del objeto seleccionado debido a los valores heredados.

Separador de tarea

Separador de tarea: **Espacio de objetos**

Tarea de gestión

El panel de la tarea de gestión Espacio de objetos proporciona tres vistas de información distintas que se seleccionan desde los separadores secundarios del panel.

- Vista **ACL heredadas** (valor por omisión)

  Esta es la vista por omisión. Visualiza la cadena de ACL que afecta al objeto seleccionado. Una flecha señala siempre a la ACL que afecta inmediatamente al objeto seleccionado en la vista de árbol Espacio de objetos.
- Vista **Editar ACL**

  Esta vista muestra la parte del panel de gestión de ACL que permite modificar directamente los atributos de las ACL.
- Vista de árbol **Valores heredados**

  Esta vista muestra una vista de árbol de la cadena de valores heredados de ACL que afecta directamente al objeto seleccionado.

Botones de acción

Los botones de acción de **Espacio de objetos** son:

- Unir ACL
- Eliminar ACL
- Buscar ACL
- Guardar ACL
- Listar

Tarea de gestión de Usuario proxy

Policy Director, combinado con un sistema cortafuego de la empresa puede proteger totalmente la intranet de una compañía contra accesos e intrusiones no autorizados. El panel de la tarea de gestión Usuario proxy permite crear y mantener usuarios proxy en el dominio seguro. Cuando se selecciona un usuario proxy desde la vista de árbol, los campos de la vista de detalles se rellenan con los datos actuales.

Separador de tarea

Separador de tarea: **Usuario proxy**

Tarea de gestión

El panel de la tarea de gestión Usuario proxy contiene una vista de lista Usuarios proxy y una vista de detalles Detalles de usuario proxy.

El panel de la tarea de gestión Detalle de usuario proxy contiene campos que visualizan la información de usuario proxy por omisión.

Botones de acción

Los botones de acción de **Usuario proxy** son:

- Guardar
- Eliminar

Propiedades y controles de Management Console

Management Console requiere la utilización del cliente Policy Director NetSEAT en Microsoft Windows NT 95 o 98 para efectuar las tareas de gestión a través de canales de comunicación seguros. En AIX y Solaris, Management Console utiliza el cliente DCE del sistema para ejecutar las tareas de gestión.

Arrastrar y soltar

Muchas de las operaciones de Management Console pueden realizarse utilizando el ratón para arrastrar objetos de una ubicación y soltarlos en otra. Por ejemplo, puede añadir un usuario a un grupo arrastrando el icono **Usuario** de la Lista de usuarios. Después, únicamente deberá soltarlo en la vista de árbol Grupos.

La forma del cursor cambia para convertirse en una mano cuando se encuentra sobre un icono que puede arrastrarse.

Pueden arrastrarse y soltarse los siguientes objetos:

- Usuario
- Grupo
- ACL
- Entrada de ACL
- Objetos del espacio de nombres
- Recursos GSO y Grupos de Recursos GSO
- Usuario proxy

Nota: Todas las operaciones de soltar que causan una actualización de la base de datos producen un recuadro de diálogo de confirmación-alerta.

Con el método de arrastrar y soltar se pueden efectuar consultas de datos. Por ejemplo, cuando se arrastra un icono **ACL** del tablón de anuncios hasta la vista Definición de ACL, los campos se rellenan con los datos actuales.

Si suelta un objeto (icono) en una ubicación que no acepta esa operación, el objeto (icono) volverá al lugar de origen.

Nota: Las operaciones de arrastrar y soltar sólo funcionan en el contexto de Management Console.

Realización de actividades en los paneles superior e inferior

Las operaciones de actualización de Management Console se efectúan en los paneles superior e inferior. Se pueden arrastrar objetos del panel inferior y soltarlos en el panel superior. Guarde en la base de datos las modificaciones realizadas en cualquiera de los dos paneles.

Policy Director sincroniza siempre la información de ACL visualizada en el panel Espacio de objetos y en el panel ACL.

Selección de varios elementos de una lista

Puede seleccionar elementos de listas y tablas utilizando las siguientes técnicas estándar de selección de Windows:

- Con una sola pulsación del botón sobre un elemento se selecciona dicho elemento.
- Mantenga pulsada la tecla Control para seleccionar más elementos al mismo tiempo.
- Una pulsación del botón seguida de Desplazamiento + pulsación selecciona el bloque de texto entre las dos pulsaciones.
- Todos los elementos de una lista pueden seleccionarse utilizando **Control + a**.

Edición de un campo de entrada de datos

Cuando edite un campo de entrada de datos, recuerde que:

- Puede utilizar la tecla Intro para activar y desactivar un campo de edición de texto.
- Puede utilizar la tecla Esc para restaurar la anterior entrada de datos en un campo que esté editando.
- En las máquinas cliente de Windows, puede utilizar las pulsaciones de teclas estándar de Windows para efectuar operaciones de copiar, cortar y pegar específicas de Management Console.
- Después de salir de un campo en el que se hayan modificado datos, aparecerá un indicador rojo en el ángulo superior izquierdo de la vista. Pulse el botón **Guardar** para confirmar todos los cambios en la base de datos.
- Puede utilizar la operación de arrastrar y soltar para rellenar algunos campos de datos.

Consultas de listas

Se pueden efectuar consultas en muchas de las vistas de listas. El icono de consulta aparece en el ángulo superior izquierdo de la ventana de la vista de lista.

Navegación

Para navegar entre campos:

- En una vista de detalles, el tabulador desplaza el cursor de un campo de entrada de datos al siguiente.
- Cuando el cursor se encuentra en el último campo de una vista de detalles, el tabulador desplaza el cursor a la siguiente vista. El cursor se desplaza de izquierda a derecha.
- Cuando el cursor se encuentra en una vista de lista o de árbol, el tabulador desplaza el cursor a la siguiente vista. El cursor se desplaza de izquierda a derecha.

- Desplazamiento + Tabulador desplaza el cursor a la siguiente vista de derecha a izquierda.
- La tecla Inicio lleva el cursor al principio de una vista. La tecla Fin lleva el cursor al final de la vista.

En una vista de detalles, las teclas Inicio + Fin llevan el cursor al principio y al final de la vista cuando todos los campos están inactivos. Si algún campo está activo, Inicio + Fin llevarán el cursor al principio y al final del campo activo.

Utilización de iconos de objetos

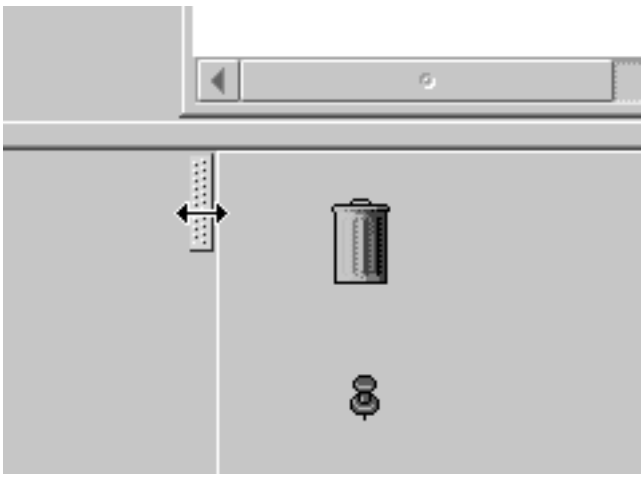
Cuando utilice iconos de objetos, recuerde que:

- Un icono exclusivo representa gráficamente a cada tipo de objeto en el espacio de nombres.
- Cada tabulador de tarea visualiza el icono del objeto afectado por esa tarea de gestión.
- Las vistas de detalles visualizan el icono del objeto que se está editando en el ángulo superior izquierdo de la vista.
- La operación de arrastrar y soltar visualiza el icono del objeto seleccionado.
- Un objeto debe arrastrarse utilizando su icono.
- La forma del cursor cambia para convertirse en una mano cuando se encuentra sobre un icono que puede arrastrarse.

Cambio del tamaño de las vistas utilizando el icono separador

Todos los paneles de tareas de gestión contienen una o más vistas. Utilice el icono separador que se encuentra en la parte superior del borde izquierdo de la vista para cambiar el tamaño de la misma. También se puede cambiar el tamaño de las columnas de las vistas de lista colocando el cursor en el icono separador entre dos cabeceras de columnas.

Cuando se mueve el cursor por el separador, su forma cambia y se convierte en una doble flecha que indica que puede cambiarse el tamaño de la vista.



Clasificación de listas

Pulsando el botón en la barra de título de la columna, puede cambiar la clasificación de la información de las vistas de lista, que puede ser ascendente o descendente. Un icono a la derecha de la barra de título indica el orden de clasificación actual.

Los elementos seleccionados en una lista siguen seleccionados después de clasificar la lista.

Ampliación y reducción de las vistas de árbol

Una vista de árbol es parecida a la visualización de archivos y directorios del Explorador de Microsoft Windows®. Para poder ampliar o reducir un nodo, debe ver un icono—un recuadro— con un signo más o un signo menos. Efectúe una doble pulsación en este icono para pasar de una vista de árbol ampliada a una reducida y viceversa. El equivalente en el teclado es **Control + e**.

Si un nodo no tiene objetos ni nodos bajo él, el indicador de ampliación/reducción desaparecerá después de pulsar sobre él.

Se puede renovar todo el árbol ampliando y reduciendo el nodo root.

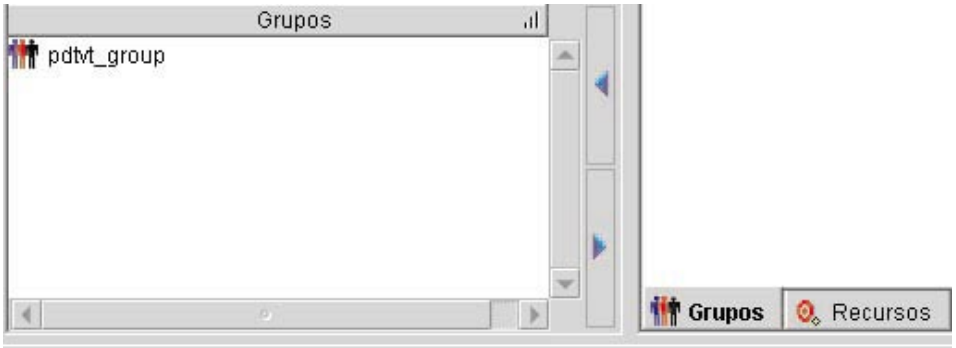
Utilización de flechas del nodo de desplazamiento del espacio de objetos

La barra de título de la vista **Espacio de objetos** contiene dos flechas azules. Estas dos flechas azules permiten limitar el foco de la vista de árbol a una rama del árbol.

- **Flecha izquierda** — esta flecha desplaza el nodo u objeto seleccionado y lo alinea completamente a la izquierda de forma que aparezca en la posición del root.
- **Flecha derecha** — esta flecha desplaza los nodos del árbol hacia atrás (un nodo con cada pulsación del botón). Después de utilizar la flecha izquierda, utilice la derecha (una o más pulsaciones) para devolver al árbol su orientación normal.

Utilización de flechas de selección

Las flechas de selección trasladan la información seleccionada de una vista de ventana a otra vista de ventana. Esto se hace para introducir nueva información en el campo de la segunda ventana.



Capítulo 5. Gestión de cuentas de usuarios y de grupos

El modelo de seguridad de Policy Director requiere la autentificación de la identidad de un usuario antes de autorizarlo a acceder a un objeto. Las autentificaciones de identidades de usuarios pueden realizarse comparando identidades de usuario y contraseñas cifradas con información de cuentas de una base de datos primaria de registros. Por omisión, Policy Director utiliza el registro LDAP. Un administrador de seguridad puede utilizar Management Console para crear y gestionar los usuarios y grupos que participan del dominio seguro.

Este capítulo incluye los siguientes temas:

Qué son usuarios, grupos y cuentas

El servicio de seguridad de Policy Director se basa en un registro primario de contabilidad—una base de datos que contiene información sobre usuarios, grupos y cuentas del dominio seguro. Por omisión, Policy Director utiliza el registro LDAP.

Usuarios

Los *usuarios* son los principales o participantes del dominio seguro. Los usuarios pueden ser personas, procesos de servidor, máquinas u otros dominios seguros.

Un usuario es una entidad que puede participar con otro usuario en un intercambio de autentificación. *La autentificación* es el proceso en que se comprueba si un usuario es quien dice ser. Todos los usuarios tienen una contraseña (o clave secreta) que se utiliza para la autentificación.

Los usuarios pueden asociarse a permisos de control de acceso. Cada usuario tiene su propio identificador exclusivo universal (Universal Unique Identifier, UUID) que es siempre el mismo, incluso si el nombre del usuario cambia. Policy Director pasa el UUID al servicio de seguridad como credencial de seguridad.

Grupos

Los *Grupos* son conjuntos de usuarios que se identifican mediante un nombre de grupo. Los grupos pueden representar distintos niveles de funciones de seguridad o de responsabilidad. Con fines de seguridad, Policy Director trata exactamente igual a todos los usuarios que son miembros de un mismo grupo. Un usuario puede pertenecer a más de un grupo, dependiendo de sus funciones y obligaciones.

Los grupos facilitan la administración y la gestión de la política de seguridad. Utilice ACL para definir la política de seguridad de un grupo. Cuando se modifiquen la función, responsabilidad o existencia de un usuario, también deberán modificarse todas las entradas de dicho usuario en las ACL. Sin grupos, la modificación de las ACL que contengan entradas para ese usuario individual sería una tarea prácticamente imposible.

Una entrada de grupo en la ACL puede representar la función o responsabilidad del usuario. Si es así, la única gestión necesaria será añadir o suprimir la pertenencia del usuario al grupo.

Los grupos, como los usuarios, tienen UUID además del nombre de grupo. El UUID de grupo es un componente de las credenciales de seguridad del usuario.

Cuentas

Una *cuenta* es una relación que implica a un usuario, a los grupos asociados y a la información de seguridad pertinente. En el registro, una cuenta define la identidad de un usuario en la red. Las cuentas definen una identidad en la red asociando un usuario a uno o más grupos y a información de seguridad pertinente como, por ejemplo, la contraseña que se utiliza para la autentificación.

Debe crearse una cuenta para cada usuario que inicie una comunicación en el dominio seguro, independientemente de si la comunicación se ha autentificado.

Se pueden asociar cuentas de usuario con la contraseña del usuario y con la información que se utilice cuando el usuario inicia la sesión con el dominio seguro. La información de la cuenta puede incluir el directorio inicial, el shell de inicio de sesión y la norma de autentificación (contraseñas) del usuario. Esta información ayuda a controlar el acceso de un usuario al dominio seguro.

Nota: Es necesario añadir un grupo al registro antes de utilizarlo en una cuenta de usuario.

Gestión de grupos

Un grupo es un conjunto de uno o más usuarios. Normalmente, los grupos se crean para indicar departamentos comunes de una empresa (por ejemplo, ventas, formación y departamento técnico). También se pueden crear categorías de grupo basadas en los distintos trabajos (por ejemplo, administradores del sistema o un grupo de usuarios que realicen copias de seguridad rutinarias).

Las categorías de grupos pueden simplificar la gestión del control de accesos dentro del dominio seguro de Policy Director. Se permite el acceso de nuevos usuarios a la información asignándoles la pertenencia a un grupo de la categoría de grupo adecuada. Este método elimina la necesidad de crear nuevas entradas de ACL para cada nuevo usuario.

Por ejemplo, cuando un nuevo empleado se una al departamento técnico, se creará una nueva cuenta de usuario que incluya su pertenencia al grupo en la categoría de `técnicos`. El nuevo usuario podrá leer entonces todos los documentos técnicos que el grupo `técnicos` tenga autorización para leer. No será necesario crear una nueva entrada de ACL para ese usuario en la plantilla de ACL ″técnicos″.

Management Console se utiliza para añadir, modificar o eliminar entradas de grupos en el registro de seguridad de Policy Director.

Después de haber creado una o más entradas de grupo, se pueden asignar usuarios a grupos. Un usuario puede pertenecer a más de un grupo, dependiendo de sus distintas funciones y obligaciones.

Utilización del panel de gestión Grupos

El administrador de seguridad del dominio seguro utiliza Management Console para crear grupos:

1. Inicie la sesión con Management Console como administrador, por ejemplo `cell_admin`.
2. Pulse el botón en el separador de tarea **Grupos**.

   Se visualizará el panel de la tarea de gestión Grupos.

Utilización de botones de acción para tareas de gestión de grupos

Los botones de acción de **Grupos** se utilizan para realizar operaciones de gestión de grupos. La siguiente tabla describe las tareas que realiza cada botón de acción:

Botón de acción	Descripción
Nuevo	Crea una nueva entrada de grupo para el dominio seguro.
Obtener	Recupera información sobre un grupo indicado específicamente y rellena las ventanas de vistas de detalles.
Guardar	Guarda esta entrada de grupo. La nueva entrada aparece en la ventana de lista adecuada.
Eliminar	Elimina el grupo seleccionado de la base de datos de registros.

Utilización de los campos de detalle de grupos

La siguiente tabla describe los campos que se encuentran en la vista **Detalle de grupo** de Management Console:

Campo	Descripción
Nombre de grupo	El nombre primario asignado a un grupo del dominio seguro. El Nombre de grupo es un campo clave que se utiliza para efectuar las consultas en el registro.
Descripción	El texto informativo que describe el grupo. La Descripción es únicamente un campo de datos opcional y el registro no lo utiliza.
LDAP	Para LDAP: • Como cn =, escriba un nombre común como, por ejemplo, `credit` • Como dn =, escriba un nombre distinguido, como por ejemplo, `cn=credit Lucas,o=IBM,ou=Austin,c=US`

Creación de un nuevo grupo

Para crear un nuevo grupo:

1. Pulse el botón del ratón en el botón de acción **Nuevo**.

   Active los campos de entrada para **Nombre de grupo** y **Descripción** en el área de Detalle de grupo.
2. Escriba el nombre del nuevo grupo y, si lo desea, escriba también una descripción del grupo en el campo **Descripción**.
3. Añada la información necesaria del registro LDAP si LDAP es el registro por omisión.
4. Se pueden añadir usuarios al nuevo grupo arrastrando iconos de usuario de la vista de lista ID de usuario y soltándolos en la ventana ID de usuario de la vista Detalle de grupo.

Asimismo, puede utilizar flechas de selección para introducir y extraer usuarios del panel ID de usuario.

5. Pulse el botón del ratón en el botón de acción **Guardar**.

   En la vista de lista Grupos aparecerá una nueva entrada de grupo.

Modificación de detalles de grupo

Para cambiar la pertenencia a un grupo o el nombre de un usuario en un grupo existente:

1. Seleccione un grupo de la vista de lista Grupos.

   La vista Detalle de grupo se rellenará con la información actual acerca del grupo.
2. En el área de Detalle de grupo, seleccione el campo que desea modificar (consulte el apartado “Utilización de los campos de detalle de grupos” en la página 73) y entre los nuevos valores.
3. También puede añadir nuevos usuarios al grupo o suprimir usuarios del grupo.

   En la columna ID de usuario, efectúe una doble pulsación en el icono de un usuario. A continuación, arrastre y suelte el nombre del nuevo usuario en la ventana ID de usuario de la vista Detalle de grupo. También puede utilizar las flechas de selección.
4. Pulse el botón **Guardar**.

Eliminación de un grupo

Para eliminar un grupo

1. En la vista de lista Grupos, seleccione el nombre del grupo que desea eliminar.

   La lista de miembros del grupo aparece en la vista Detalle de grupo.
2. Seleccione los miembros del grupo, de uno en uno, y elimínelos del grupo también de uno en uno.
3. En la vista de lista Grupos, seleccione el grupo.
4. Pulse el botón **Eliminar** para eliminar completamente la entrada correspondiente al grupo.

Gestión de cuentas de usuarios

Los usuarios que soliciten acceso a los servicios y objetos del dominio seguro deberán autentificarse a sí mismos ante Policy Director. Todos los usuarios que deseen participar del dominio seguro de Policy Director deberán tener registrada una cuenta con LDAP.

Utilización del panel de gestión de usuarios

El administrador de seguridad del dominio seguro utiliza Management Console para crear cuentas de usuarios:

1. Inicie la sesión con Management Console como administrador, por ejemplo `cell_admin`)
2. Pulse el botón en el separador de tarea **Usuarios**.

   Aparecerá el panel de tarea de gestión Usuarios.

Utilización de los botones de acción para tareas de gestión de usuarios

Para llevar a cabo las operaciones de gestión de Usuarios se utilizan los botones de acción de **Usuarios**. La siguiente tabla describe las tareas que realiza cada botón de

acción:

Botón de acción	Descripción
Nuevo	Crea una nueva cuenta de usuario para el dominio seguro.
Obtener	Recupera información sobre un usuario indicado específicamente y rellena las ventanas de vistas de detalles.
Guardar	Guarda la cuenta de ese usuario. La nueva entrada aparece en la ventana de lista adecuada.
Eliminar	Elimina el usuario seleccionado de la base de datos de registros.

Utilización de los campos de detalle de usuarios

La siguiente tabla describe los campos que se encuentran en la vista **Detalle de usuario** de Management Console:

Campo	Descripción
ID de usuario	El nombre primario asignado a un usuario del dominio seguro. El ID de usuario es un campo clave que se utiliza para efectuar las consultas al registro.
Descripción	El texto informativo que describe al usuario. La Descripción es únicamente un campo opcional y el registro no lo utiliza.
Cuenta válida	Este recuadro de selección permite controlar la posibilidad de que un usuario de participe (o no) en el dominio seguro. Cuando se borra el recuadro, la cuenta deja de ser válida. No obstante, la información de la cuenta sigue permaneciendo en el registro.
Contraseña válida	Este recuadro de selección permite forzar un cambio de contraseña la siguiente vez que el usuario inicie la sesión con el dominio seguro. Cuando se borra el recuadro, el usuario recibe una notificación indicándole que su contraseña ha caducado.
Usuario GSO	Este recuadro de selección indica que el usuario tiene la posibilidad de utilizar GSO.
LDAP	Para LDAP: • Como cn=, escriba un nombre común como, por ejemplo, `"Diana Lucas"` • Como sn= , escriba un alias como, por ejemplo, `Lucas` • Como dn=, escriba un nombre distinguido, como por ejemplo, `cn=Diana Lucas,o=IBM,ou=Austin,c=US`

Adición de una nueva cuenta de usuario

Para añadir una nueva cuenta de usuario:

1. Pulse el botón del ratón en el botón de acción **Nuevo**.

   En la vista Detalle de usuario aparecerán campos de entrada en blanco.
2. Escriba los datos adecuados en los campos. En el apartado “Utilización de los campos de detalle de usuarios” encontrará la información completa sobre estos campos.

   Puede arrastrar y soltar un icono de **grupo** desde la vista de árbol Grupos para rellenar la ventana Miembro de grupos—o utilizar las flechas de selección.
3. Añada la información necesaria del registro LDAP si LDAP es el registro por omisión.
4. Pulse el botón en **Guardar**.

Modificación de las propiedades de cuentas

Para modificar las propiedades de una cuenta existente:

1. Seleccione el usuario de la vista de lista ID de usuario.
   El área Detalle de usuario se rellena con los datos actuales.
2. En la vista Detalle de usuario, pulse el botón en el campo que desee modificar.
3. Entre los nuevos datos.
4. Pulse el botón en **Guardar**.

Eliminación de una cuenta de usuario

Para eliminar una cuenta de usuario:

1. Seleccione el usuario de la vista de lista ID de usuario.
2. Pulse el botón en **Eliminar**.

Creación de varias cuentas de administración

Un usuario de administración debe estar en los siguientes grupos. Cuando pertenece a dichos grupos, el usuario de administración tiene autorización para añadir, modificar o eliminar usuarios, grupos y organizaciones que se encuentren en el dominio seguro.

- acct-admin
- subsys/dce/sec-admin
- subsys/dce/cds-admin

Cuando se crea inicialmente un dominio seguro, la única cuenta que contiene esa combinación de grupos es cell_admin.

Cuando un dominio seguro alcanza un determinado tamaño es problemático para el administrador gestionar el número creciente de tareas. La gestión de un dominio seguro grande requiere la delegación de responsabilidades administrativas.

Se pueden crear más cuentas de administración que tengan las mismas posibilidades de operar con Management Console asignándoles la pertenencia a los grupos del árbol listados. La planificación y organización de la delegación de autoridad debe coincidir con la creación de esas cuentas.

Importación de información de otras fuentes

Se puede rellenar el registro con datos de usuarios y de grupos de otras fuentes.

Capítulo 6. Gestión de recursos GSO, grupos de recursos y credenciales de recursos

Policy Director tiene soporte para una solución de conexión más flexible gracias a la integración de la tecnología IBM Global Sign-On (GSO). La integración se consigue creando conexiones Smart Junction de Policy Director. En el apartado “Capítulo 15. WebSEAL: administración de Smart Junction” en la página 191 encontrará información detallada sobre las Smart Junction.

Cuando WebSEAL recibe una petición para un recurso situado en el servidor conectado (″junction″), utiliza GSO para conseguir la información de autentificación adecuada. GSO contiene una base de datos de correlaciones para cada usuario registrado, que proporciona nombres de usuarios y contraseñas para determinados recursos y aplicaciones. Policy Director almacena los datos de GSO directamente en IBM SecureWay Directory (LDAP).

La combinación de WebSEAL y GSO proporciona una completa solución de conexión única a la Web que proporciona las ventajas adicionales que representan los datos cifrados, una alta disponibilidad y la escalabilidad.

Consulte el apartado “Integración de la conexión propia de WebSEAL y GSO” en la página 213 donde encontrará más información,

Qué son los recursos GSO y los grupos de recursos GSO

GSO contiene una *credencial de recurso* específica para el usuario que correlaciona un recurso GSO con una combinación específica de identificación de usuario (nombre de usuario) y contraseña. La credencial de recurso proporciona el nombre de usuario y la contraseña para un recurso GSO específico del usuario como, por ejemplo, un servidor Web o un grupo de servidores de la Web.

GSO proporciona información de autentificación a WebSEAL. Cuando un usuario desea ejecutar un recurso de aplicación, WebSEAL pide a GSO información sobre la autentificación del usuario. GSO mantiene una base de datos completa con información sobre autentificaciones en forma de recursos correlacionados con información de autentificación. La correlación de recursos de aplicación con el nombre de usuario y la contraseña se denomina *Credenciales de recursos GSO*. Sólo pueden crearse Credenciales de recursos GSO para usuarios registrados.

Nota: Para poder aplicar la credencial de recurso GSO, el recurso GSO o el grupo de recursos GSO deben existir.

Gestión de recursos GSO

Un *recurso GSO* es un servidor Web. Si lo desea, puede dar un nombre al recurso de la Web para identificarlo.

Utilización del panel de gestión del recurso GSO

Los recursos GSO que soliciten acceso a servicios y objetos del dominio seguro deben autentificarse ante Policy Director. Todos los recursos GSO que deseen participar del dominio seguro de Policy Director deberán tener registrada una cuenta con LDAP.

Utilización de botones de acción para tareas de gestión de recursos GSO

Los botones de acción de **Recursos GSO** se utilizan para realizar operaciones de gestión de recursos GSO. La siguiente tabla describe las tareas que realiza cada botón de acción:

Botón de acción	Descripción
Nuevo	Crea una nueva cuenta de recurso GSO para el dominio seguro.
Obtener	Recupera información sobre un recurso GSO indicado específicamente y rellena las ventanas de vistas de detalles.
Guardar	Guarda esa cuenta de recurso GSO. La nueva entrada aparece en la ventana de lista adecuada.
Eliminar	Elimina el recurso GSO seleccionado de la base de datos de registros.

Utilización de los campos de detalles de recursos GSO

La siguiente tabla describe los campos que se encuentran en la vista **Detalle de recurso** de Management Console:

Campo	Descripción
Nombre de recurso	El nombre asignado a un recurso GSO del dominio seguro. El Nombre de recurso es un campo clave que se utiliza cuando se efectúa una consulta al registro.
Descripción	El texto informativo que describe el recurso. La Descripción es únicamente un campo opcional y el registro no lo utiliza.

Adición de un nuevo recurso GSO

Para añadir un nuevo recurso GSO:

1. Pulse el botón del ratón en el botón de acción **Nuevo**.

   En la vista Detalle de recurso aparecerán campos de entrada en blanco.
2. Escriba los datos adecuados en los campos. En el apartado “Utilización de los campos de detalles de recursos GSO” encontrará la información completa sobre estos campos.

   Puede arrastrar y soltar un icono de **Grupos de recursos GSO** desde la vista de árbol Grupos de recursos para rellenar la ventana Miembro de grupos de recursos GSO—o utilizar las flechas de selección.
3. Pulse el botón del ratón en el botón de acción **Guardar**.

Creación de una credencial de recurso para el recurso GSO

Cuando haya creado la definición de recurso, podrá crear una credencial de recurso para un usuario:

Para crear una credencial de recurso:

1. Seleccione el separador **Usuarios**.
2. Seleccione el usuario para el que va a crear la credencial de recurso resaltando el nombre de usuario.
3. En la vista Detalle de usuario Recursos GSO, seleccione el separador **Recursos** para listar los recursos que estén disponibles en ese momento.
4. Seleccione el recurso al que se aplica la credencial.

5. Arrastre el recurso seleccionado al panel de recursos de la vista Detalle de usuario.

   Por omisión, los valores de ID y contraseña de inicio de sesión para la nueva credencial de recurso adoptan los mismos valores que la cuenta del cliente.
6. El ID de inicio de sesión y la contraseña pueden cambiarse para que tengan los valores adecuados para la credencial de recursos del usuario pulsando el botón en **ID de inicio de sesión** o **Contraseña** e introduciendo los valores correspondientes.
7. Pulse el botón del ratón en el botón de acción **Guardar**.

Modificación de la información sobre recursos GSO

Para modificar las propiedades de una cuenta existente:

1. Seleccione el recurso GSO de la vista de lista Recursos.

   El área Detalle de recurso se rellenará con los datos actuales.
2. En la vista Detalle de recurso, pulse el botón en el campo que desee modificar.
3. Modifique los datos existentes o entre datos nuevos.
4. Pulse el botón del ratón en el botón de acción **Guardar**.

Eliminación de un recurso GSO

Para eliminar una cuenta de usuario:

1. Seleccione el recurso GSO de la vista de lista Recursos.
2. Pulse el botón **Eliminar**.

Gestión de grupos de recursos GSO

Un *grupo de recursos* indica un grupo de servidores de la Web en el que todos los servidores del grupo tienen los mismos conjuntos de ID de usuario y contraseña.

Utilización del panel de gestión de grupos de recursos GSO

El administrador de seguridad del dominio seguro utiliza Management Console para crear grupos de recursos GSO:

1. Inicie la sesión con Management Console como administrador, por ejemplo `cell_admin`.
2. Pulse el botón en el separador de tarea **Grupos de recursos GSO**.

   Se visualizará el panel de tarea Grupos de recursos GSO.

Utilización de botones de acción para tareas de gestión de grupos de recursos GSO

Utilice los botones de acción de Grupos de recursos GSO para realizar operaciones de gestión de grupos de recursos GSO. La siguiente tabla describe las tareas que realiza cada botón de acción:

Botón de acción	Descripción
Nuevo	Crea una nueva entrada de grupo de recursos GSO para el dominio seguro.
Obtener	Recupera información sobre un grupo de recursos GSO indicado específicamente y rellena las ventanas de vistas de detalles.
Guardar	Guarda esa entrada de grupo de recursos GSO. La nueva entrada aparece en la ventana de lista adecuada.

Eliminar	Elimina el grupo de recursos GSO seleccionado de la base de datos de registros.

Utilización de los campos de detalles de grupos de recursos GSO

La siguiente tabla describe los campos que se encuentran en la vista **Nombre de grupo de recursos** de Management Console:

Campo	Descripción
Nombre de grupo de recursos	El nombre primario asignado a un grupo de recursos GSO del dominio seguro. El Nombre de grupo de recursos GSO es un campo clave que se utiliza para efectuar consultas al registro.
Descripción	El texto informativo que describe el grupo de recurso GSO. La descripción es tan solo un campo de datos opcional y el registro no la utiliza.

Adición de un nuevo grupo de recursos GSO

Para crear un nuevo grupo de recursos GSO:

1. Pulse el botón del ratón en el botón de acción **Nuevo**.

   Active los campos de entrada **Nombre de grupo de recursos** y **Descripción** en el área de Detalle de grupo de recursos.
2. Escriba el nombre del nuevo grupo de recursos y, si lo desea, escriba también una descripción del grupo de recursos en el campo **Descripción**.
3. Puede añadir recursos GSO al nuevo grupo de recursos GSO arrastrando iconos de recursos GSO desde la vista de lista Recursos GSO hasta la ventana de recursos GSO de la vista Detalle de grupo de recursos.

   Asimismo, puede utilizar flechas de selección para introducir y extraer usuarios del panel Recursos GSO.
4. Pulse el botón del ratón en el botón de acción **Guardar**.

   En la vista de lista Grupos de recursos aparecerá una nueva entrada de grupo GSO.

Creación de una credencial de recurso GSO

Se puede crear una sola credencial de recurso para todos los recursos del grupo de recursos. Policy Director utiliza una sola credencial de recurso para un grupo de recursos en vez de crear una credencial de recurso para cada recurso del grupo de recursos. Para poder crear la credencial del recurso GSO, primero debe crear el grupo de recursos.

Para crear una credencial de recurso GSO para un usuario después de haber creado la definición del grupo de recursos:

1. Elija el separador **Usuarios** y seleccione el usuario para el que desea crear la credencial de recurso.
2. En la vista Detalle de usuario Recursos GSO, seleccione el separador **Grupos de recursos** para listar los grupos de recursos que estén disponibles en ese momento.
3. Seleccione el grupo de recursos al que se aplica la credencial.
4. Arrastre el grupo de recursos seleccionado al panel Grupo de recursos de la vista Detalle de usuario.

   Por omisión, los valores de ID de inicio de sesión y contraseña para la nueva credencial de recurso adoptan los mismos valores que la cuenta del usuario.

5. El ID de inicio de sesión y la contraseña pueden cambiarse para que tengan los valores adecuados para la credencial de recursos del usuario pulsando el botón en **ID de inicio de sesión** o **Contraseña** e introduciendo los valores correspondientes.
6. Pulse el botón del ratón en el botón de acción **Guardar**.

Modificación de la información del grupo de recursos GSO

Para cambiar la pertenencia a un grupo o el nombre de un grupo de recursos existente:

1. Seleccione un grupo de la vista de vista de lista Grupos de recursos.

   La vista Detalle de grupo de recursos se rellenará con la información actual acerca del grupo de recursos.
2. En el área Detalle de grupo de recursos, seleccione el campo que desea modificar (**Nombre de grupo de recursos** o **Descripción**). Escriba los nuevos valores.
3. También puede añadir nuevos recursos al grupo o eliminar recursos del grupo.

   En la columna Grupos de recursos, efectúe una doble pulsación en el icono de un grupo de recursos. A continuación, arrastre y suelte el nuevo recurso en la ventana Recursos GSO de la vista Detalle de grupo de recursos. También puede utilizar las flechas de selección.
4. Pulse el botón del ratón en el botón de acción **Guardar**.

Eliminación de un grupo de recursos GSO

Para suprimir un grupo de recursos GSO:

1. En la vista de lista Grupos de recursos, seleccione el nombre del grupo de recursos GSO que desea eliminar.

   La lista de miembros del grupo de recursos aparecerá en la vista Detalle de grupo de recursos.
2. Seleccione los recursos GSO de uno en uno y elimínelos del grupo de recursos GSO.
3. En la vista de lista Grupos de recursos, seleccione el grupo de recursos GSO.
4. Pulse el botón en **Eliminar** para eliminar completamente la entrada correspondiente al grupo de recursos GSO.

Migración de datos GSO

Si tiene datos GSO procedentes de IBM SecureWay Global Sign-on Versión 2.0.200 o de releases anteriores de IBM Global Sign-On, necesitará migrar los datos GSO para que esta versión de Policy Director pueda utilizarlos.

La información y herramientas más recientes (por ejemplo, las herramientas de migración) se encuentran en el sitio Web de IBM SecureWay Policy Director:

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

Cambio de la contraseña de credenciales de recursos GSO

Un usuario puede actualizar la contraseña GSO almacenada de un recurso GSO o un grupo de recursos GSO utilizando la herramienta de contraseñas de Policy Director basada en la Web, chpwd.exe. Para poder utilizar esta herramienta, debe haberse creado una credencial de recurso. Utilice esta herramienta después de haber cambiado la contraseña del recurso.

Este archivo puede encontrarse en:

UNIX: `/opt/intraverse/www/docs/cgi-bin/chpwd`

Windows: `c:\Archivos de programa\www\docs\cgi-bin\chpwd.exe`

Para cambiar la credencial de recurso GSO utilizando la herramienta de la Web:

1. Abra una instancia del navegador seguro.
2. Entre la siguiente ubicación de URL:

   `https: //`*`webseal server`*`/cgi-bin/chpwd.exe`

   Donde *webseal server* es el nombre asignado a su WebSEAL Server. En Windows, escriba la extensión .exe como parte de la designación del URL.
3. Pulse el botón en el nombre del recurso en la columna Nombre de recurso para seleccionarlo.
4. Escriba su nombre de usuario en el campo **ID de usuario**.
5. Escriba la nueva contraseña que desee en el campo **Nueva contraseña**. A continuación, confírmela escribiéndola de nuevo en el campo **Confirmar nueva contraseña**.
6. Pulse el botón en **Actualizar**.

Capítulo 7. Qué es el control de acceso

Puede proteger los recursos de un dominio seguro. Los recursos se protegen definiendo normas especiales y uniendo esas plantillas a representaciones de objetos de dichos recursos. Las normas especiales se conocen como *plantillas de políticas*. Policy Director reconoce y utiliza un tipo de plantilla de política llamado *lista de control de accesos* (ACL). Utilice las ACL para estampar la política de seguridad de una empresa en los recursos que pertenecen al dominio seguro.

Este capítulo incluye los siguientes temas:

Espacio de nombres de objetos protegidos

El modelo de seguridad de Policy Director depende de normas o permisos para proteger recursos en el dominio seguro. Un conjunto específico de permisos se denomina *plantilla de política*.

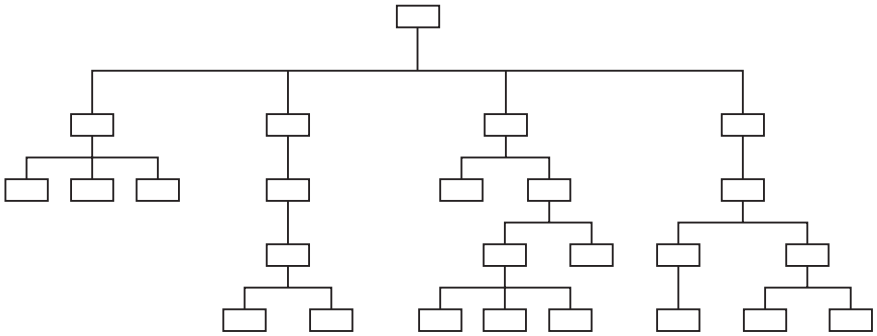
Cuando se conecta a un recurso, una plantilla de política aplica de forma eficaz la política de seguridad de la empresa al recurso. Para conseguir ese modelo de seguridad, Policy Director utiliza una representación de objeto lógico del inventario de recursos físicos del dominio seguro.

Para proporcionar protección al recurso físico actual, una las plantillas de políticas a los objetos lógicos del espacio de nombres. Policy Director Authorization Service toma decisiones de autorización comparando las credenciales de usuarios que se obtienen durante la autentificación con los permisos definidos en las plantillas.

El *espacio de nombres de objetos protegidos* de Policy Director es la descripción lógica y jerárquica de los recursos que pertenecen a un dominio seguro. Los objetos que aparecen en el espacio de nombres jerárquico representan los recursos físicos reales de la red.

Recurso del sistema
: El archivo físico, servicio de red o aplicación reales.

Objeto protegido
: La representación lógica de un recurso real del sistema utilizado por Policy Director Authorization Service, Management Console y demás programas de utilidad de gestión de Policy Director.



El espacio de nombres de objetos protegidos utiliza dos tipos de objetos:

Objetos contenedores
Los objetos contenedores son designaciones estructurales que permiten organizar el espacio de nombres jerárquicamente en distintas regiones funcionales. Los objetos contenedores contienen objetos de recursos.

Objetos de recursos
Los objetos de recursos son las representaciones de recursos de red reales (como servicios, archivos y programas) en el dominio seguro.

Jerarquía del espacio de nombres de objetos protegidos

El principio estructural del espacio de nombres de objetos protegidos es el objeto contenedor **root**. En Policy Director Management Console, el símbolo del root es la barra inclinada (/).

Las siguientes categorías del espacio de nombres siguen al objeto root:

objetos de la Web (contenedor /WebSEAL)
El objeto de contenedor WebSEAL es el root lógico de espacio de la Web del dominio seguro. Policy Director autoriza todas las operaciones HTTP para determinados objetos de este subárbol.

Los *objetos de la Web* representan todo lo que un URL puede dirigir, incluidas páginas Web estáticas y URL dinámicos. Las pasarelas de Web a aplicación convierten las páginas Web estáticas o los URL dinámicos en consultas a la base de datos o en cualquier otro tipo de llamada de aplicación.

Objetos de aplicaciones de la red (contenedor /NetSEAL)
El objeto del contenedor NetSEAL es el root del espacio lógico que contiene los servicios protegidos de NetSEAL en el dominio seguro. Estos objetos representan aplicaciones basadas en TCP (como TELNET y FTP) que se correlacionan con direcciones TCP de la red (puertas). La aplicación utiliza esas puertas.

Objetos de gestión de Policy Director (contenedor /Management)
El objeto del contenedor Management es el root del espacio lógico que controla todas las operaciones de gestión de Policy Director. Los objetos de gestión representan los servicios necesarios para definir usuarios y establecer políticas de seguridad. Realice esas tareas utilizando Policy Director Management Console o el programa de utilidad **ivadmin**.

Las subdivisiones de esta región incluyen:

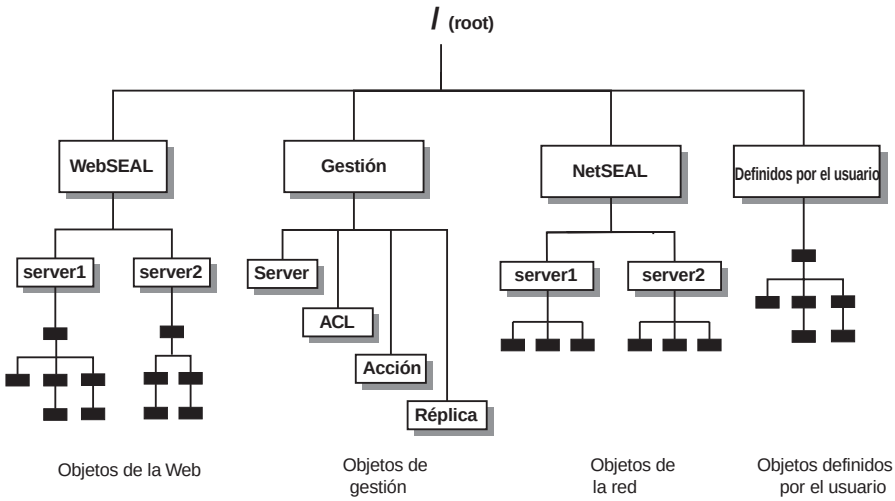
- Tareas de gestión del servidor (/Server)
- Tareas de política de seguridad (/ACL)

- Control de autorizaciones de terceros (/Action)
- Control de réplicas de la base de datos de autorizaciones (/Replica)

Policy Director permite la delegación de actividades de gestión y pueden restringir la posibilidad de un administrador de establecer políticas de seguridad a un subconjunto del espacio de nombres.

Objetos definidos por el usuario

Estos objetos representan tareas o recursos de la red protegidos por aplicaciones de terceros que utilicen Policy Director Authorization Service, que a su vez utiliza la API de autorizaciones de Policy Director.



Espacios de nombres de aplicaciones de terceros

Policy Director puede facilitar servicios de autorizaciones a cualquier objeto de aplicación que esté definido por el espacio de nombres de objetos protegidos. Las aplicaciones que forman parte de la familia Policy Director incluyen WebSEAL (para aplicaciones de la Web) y NetSEAL (para aplicaciones basadas en TCP).

Policy Director y las aplicaciones de terceros efectúan llamadas a Policy Director Authorization Service a través de la API de autorizaciones de Policy Director. Para integrar una aplicación de terceros a Policy Director Authorization Service, lleve a cabo estos dos pasos:

1. Describa el espacio de nombres de la aplicación de terceros.
2. Aplique permisos a todos los objetos del espacio de nombres que requieran protección.

Los contenedores de objetos definidos por el usuario son regiones del espacio de nombres de objetos protegidos donde se pueden crear espacios de nombres de aplicaciones de terceros.

Es necesario definir el root (*punto de conexión Smart Junction*) en el que se inicia el espacio de nombres de terceros en el espacio de nombres de objetos protegidos. En el apartado “Definición de espacios de nombres de aplicaciones de terceros” en la página 135 encontrará información más detallada.

Después podrá utilizar Management Console o el programa de utilidad **ivadmin** para crear, unir y eliminar ACL en los objetos de este nuevo espacio de nombres.

Listas de control de acceso

Una *lista de control de accesos* (ACL) es el tipo de plantilla de política utilizado por Policy Director para proporcionar protección a los recursos del dominio seguro.

Una ACL es un conjunto de normas o permisos que especifican las condiciones necesarias para realizar una operación en un recurso protegido. Las ACL identifican las operaciones permitidas sobre recursos protegidos y listan las identidades (usuarios, grupos o ambos) que pueden realizar dichas operaciones, por ejemplo:

- Definiciones de identidades de usuarios e identidades de grupos en el registro de seguridad.
- Definiciones del espacio de nombres de objetos protegidos y de las plantillas de políticas de la base de datos de políticas de autorización.

Como plantilla de política cada ACL de Policy Director tiene un nombre exclusivo o *etiqueta* que indica la política de seguridad que representa. A continuación, aplique las ACL a las representaciones de objetos de los recursos del espacio de nombres de objetos protegidos.

Una ACL está formada por una o más entradas que incluyen designaciones de usuario y designaciones de grupo y sus permisos respectivos.

Entradas de ACL

Una ACL está formada por una o más entradas que describen:

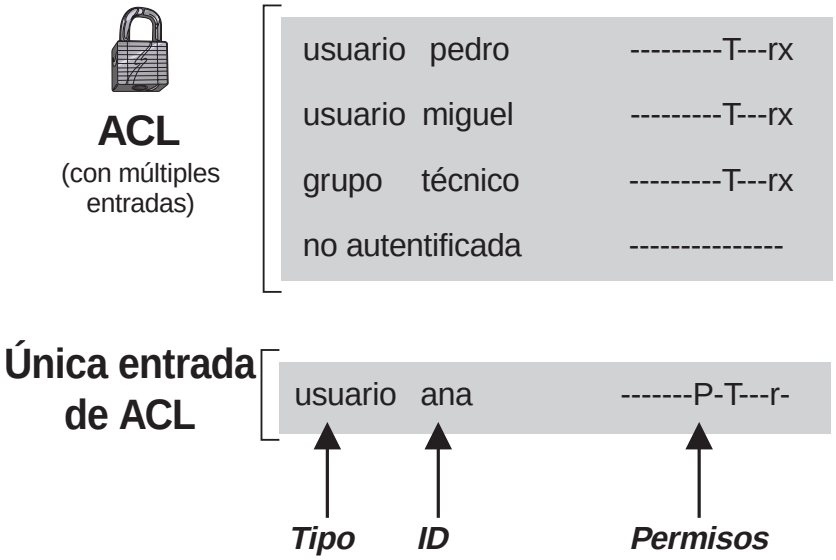
- Los UUID de los usuarios y grupos cuyo acceso al objeto está controlado explícitamente
- Las operaciones específicas que está autorizado a realizar cada usuario, grupo o función
- Las operaciones específicas que están permitidas a las categorías especiales de usuarios “cualquiera” y “no autentificado”

Un *usuario* o principal representa a cualquier identidad que esté autentificada por Policy Director Security Server. Normalmente, los usuarios representan a usuarios de la red o servidores de aplicaciones.

Un *grupo* es un conjunto de uno o más usuarios. Un administrador de la red puede agrupar entradas de ACL para asignar los mismos permisos a varios usuarios. Los nuevos usuarios consiguen el acceso a los objetos al convertirse en miembros de los grupos adecuados. Este método elimina la necesidad de definir nuevas entradas de ACL para cada nuevo usuario. Los grupos pueden representar divisiones o departamentos de empresas dentro de un dominio seguro. Los grupos también son útiles para la definición de funciones o asociaciones funcionales.

Colectivamente, los usuarios y grupos se consideran *entidades*.

Policy Director Management Console (separador de gestión **ACL**) se utiliza para crear, modificar y suprimir entradas de ACL.



ACL como plantillas de políticas

Management Console permite:

- Crear una ACL específica.
- Guardarla con una etiqueta.
- Aplicarla como plantilla de política de seguridad a los objetos del espacio de nombres.

La ACL se convierte en una plantilla de origen igual que, por ejemplo, un formulario o una receta. La ACL contiene las entradas específicas que proporcionan el nivel correcto de protección para todos los objetos asociados a ella.

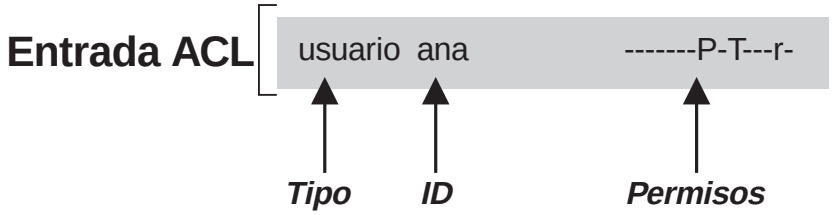
Una lista ACL de ejemplo podría incluir:

```
Nombre de ACL
    gestión por omisión
    netseal por omisión
    réplica por omisión
    root por omisión
    webseal por omisión
```

Una plantilla de ACL proporciona las mismas cualidades referidas a una sola fuente que un estilo de formateo de párrafo en un documento de proceso de texto. Si las necesidades de política de seguridad cambian, únicamente se editará la ACL sola. Policy Director pone inmediatamente en vigor la nueva definición de seguridad para todos los objetos a los que está conectada la ACL.

Sintaxis de entrada de ACL

Una entrada de ACL contiene dos o tres atributos, dependiendo del tipo de entrada de ACL y aparece con el siguiente formato:



Tipo

La categoría de la entidad (usuario o grupo) para la que se ha creado la ACL.

ID (Identidad)

El identificador (nombre) exclusivo de la entidad.

Los tipos de entrada de ACL ″autentificada por cualquiera″ o no autentificada″ no requieren el atributo ID.

Permisos

El conjunto de operaciones sobre el objeto para las cuales tiene permiso el usuario o grupo.

La mayoría de los permisos indican la posibilidad del cliente de realizar una operación específica sobre el recurso. Varios de los permisos imponen determinadas condiciones siempre que se permite la ejecución de una acción sobre un recurso. Por ejemplo, al forzar el cifrado de los datos, al requerir la protección de la integridad de los datos, al escribir un registro de informe en el servicio de auditoría o cuando se requiere alguna condición de autorización externa.

En este ejemplo, Ana (tipo=usuario, ID=ana) tiene permiso para leer (visualizar) el objeto asociado a la ACL que contiene esta entrada. La autorización de lectura (r) permite efectuar la operación de lectura. El permiso de cifrado (P) obliga a que los canales de comunicaciones utilicen el cifrado de los datos. El permiso de atravesar (T) impone el atributo de atravesar.

Atributo de tipo

Un tipo de entrada de ACL indica la entidad correspondiente a la entrada de ACL. Hay cuatro tipos de entradas de ACL:

Tipo	Descripción
usuario	Define permisos para un usuario específico del dominio seguro. El tipo de entrada de usuario requiere un nombre (ID) de cuenta. El formato de la entrada es `ID de usuario permisos`. Por ejemplo: `usuario laura ----------r-`

grupo	Define permisos para miembros de un grupo específico del dominio seguro. El tipo de entrada de grupo requiere un nombre (ID) de grupo. El formato de la entrada es `ID de grupo permisos`. Por ejemplo: `grupo técnico ----------r-`
autentificado por cualquiera	Define permisos para todos los usuarios autentificados. No es necesario indicar ningún ID. El formato de la entrada es: `autentificado por cualquiera ----------r-`

no autentificado	Define permisos para los usuarios que no han sido autentificados por Security Server. No es necesario indicar ningún ID. El formato de la entrada es: `no autentificados permisos`. Por ejemplo:
	`no autentificados ---------T---r-`
	
	Esta entrada de ACL es una máscara (una operación “and” de bit) para la entrada de ACL autentificada por cualquiera a fin de determinar el permiso definido. Por ejemplo, la siguiente entrada de ACL no autentificada:
	`no autentificados ----------r-`
	
	enmascarada para esta esta entrada de ACL autentificada por cualquiera:
	`autentificado por cualquiera ---------T---r-`
	
	da como resultado estos permisos:
	`----------r- (sólo lectura).`

Atributo de ID

El ID de ACL es el *identificador exclusivo*, o nombre para los tipos de entrada de usuario o entrada de grupo. Los ID deben representar usuarios y grupos válidos que se hayan creado para el dominio seguro y se hayan almacenado en la base de datos de registros.

A continuación puede ver ejemplos de identificadores exclusivos:

```
usuario miguel
usuario laura
grupo técnico
grupo documentación
grupo contabilidad
```

Nota: No utilice el ID de atributo para los tipos de entrada de ACL autentificada por cualquiera y no autentificada.

Atributos de permisos

Cada entrada de ACL contiene un conjunto de *permisos* que describen:

- Las operaciones específicas que puede realizar el usuario o el grupo sobre el objeto.
- Todas las limitaciones sobre el tipo de acceso al objeto como, por ejemplo:
  - Utilización obligatoria de privacidad o integridad de los datos en el canal de comunicaciones
  - Acceso auditado

– Requisitos de autorización externa (de terceros)

Las ACL controlan los recursos protegidos controlando:

- La posibilidad de un usuario de realizar operaciones sobre objetos protegidos
- La posibilidad de un administrador de cambiar las normas de control de accesos al objeto y a los subobjetos que pueda haber
- La posibilidad de Policy Director Server de delegar credenciales de usuario

Secuencia de permisos

Los permisos de ACL son *sensibles al contexto*. Los permisos sensibles al contexto son aquellos en los que el comportamiento de determinados permisos varía. El comportamiento varía con arreglo a la región del espacio de objetos protegidos en la que se aplica. Por ejemplo, el permiso m tiene un significado distinto en un objeto WebSEAL y en un objeto Management.

Los diecisiete permisos estándar están agrupados en cuatro categorías y aparecen en el siguiente orden cuando se utilizan en una entrada de ACL:

Base	Genérico	NetSEAL	WebSEAL
a A b c g I P T	d m s v	C p	l r x

La ventana Definición de ACL/Entrada de ACL visualiza la lista de permisos entre los que puede escogerse. Seleccione los recuadros de selección que aparecen al lado de los permisos para seleccionarlos:

Base
(a) Unir
(A) Auditoría
(b) Examinar
(c) Controlar
(g) Delegación
(I) Integridad
(P) Privacidad
(T) Atravesar
Genérico
(d) Eliminar
(m) Modificar
(s) Admin servidor
(v) Visualizar
NetSEAL
(C) Conectar
(p) Proxy
WebSEAL
(l) Directorio de lista
(r) Leer
(x) Ejecutar

Regiones del espacio de nombres

Los objetos contenedores representan regiones específicas del espacio de nombres de objetos protegidos y se aplican a estas importantes funciones de seguridad:

1. Se puede utilizar la ACL de objeto contenedor para definir políticas de alto nivel para todos los subobjetos de la región cuando no se aplica ninguna otra ACL explícita.
2. Se puede utilizar la ACL de objeto contenedor para definir políticas de alto nivel para todos los subobjetos de la región. Una política de alto nivel puede definirse cuando no se aplica ninguna otra ACL explícita.

3. El acceso a todos los objetos de una región se puede denegar rápidamente eliminando el permiso de atravesar de la ACL del objeto contenedor.

Permiso de atravesar

El permiso de atravesar es un permiso genérico que se aplica en todo el espacio de nombres de objetos protegidos:

Permiso de atravesar:	**Acceso**	**Descripción**
T	atravesar	Permite al solicitante pasar jerárquicamente a través del objeto en su camino hacia el objeto solicitado. No permite ningún otro tipo de acceso al objeto. El permiso de atravesar también es necesario para el objeto propiamente dicho.

Condiciones de acceso

Las condiciones de acceso son permisos genéricos que se aplican en todo el espacio de nombres de objetos protegidos:

Condiciones de acceso para todos los objetos protegidos:	**Acceso**	**Descripción**
A	auditoría	Hace que Policy Director Server grabe un registro de auditoría en el servicio de auditoría siempre que se accede al objeto. Se auditan todos los intentos de acceso, incluidos aquellos en que no se otorga la autorización
I	integridad	Para acceder a este objeto, se requiere protección de integridad de datos entre el cliente y Policy Director Server
P	privacidad	Para acceder a este objeto, se requiere el cifrado de datos entre el cliente y Policy Director Server

Permiso de control

El permiso de control es una potente autorización que otorga la propiedad de la ACL. El control permite modificar las entradas de la ACL. Teniendo el control se puede crear entradas, eliminar entradas, otorgar permisos y revocar permisos.

Permiso de control:	**Acceso**	**Descripción**
c	control	Propiedad de la plantilla de ACL; se pueden crear, eliminar y modificar entradas para esta ACL.

El administrador puede eliminar esta ACL de la lista de plantillas de ACL. Para poder efectuar la supresión, el administrador debe tener una entrada en la ACL y debe tener un permiso de control definido en dicha entrada.

El permiso de control permite otorgar facultades de administración a otro usuario. Por ejemplo, se le puede permitir que conecte una ACL a objetos. Una ACL se conecta a objetos utilizando el permiso de conexión (a).

El permiso de control (c) debe utilizarse con mucho cuidado debido a sus potentes facultades de propiedad.

Objeto contenedor root

Las siguientes consideraciones sobre seguridad se aplican al objeto contenedor *root* (/):

- El objeto root inicia la cadena de valores heredados de ACL para todo el espacio de nombres de objetos protegidos.
- Si no se aplica ninguna otra ACL explícita, el objeto root define (mediante valores heredados) la política de seguridad de todo el espacio de nombres.
- Para acceder a cualquier objeto que se encuentre por debajo del root, deberá utilizar el permiso de atravesar (T).

Espacio de nombres WebSEAL

Las siguientes consideraciones sobre seguridad se aplican al objeto contenedor /WebSEAL:

- El objeto WebSEAL inicia la cadena de valores heredados de ACL para la región WebSEAL del espacio de nombres.
- Si no se aplica ninguna otra ACL explícita, este objeto define (mediante valores heredados) la política de seguridad de todo el espacio de la Web.
- Para acceder a este objeto y a cualquier otro que se encuentre por debajo de este punto, deberá utilizar el permiso de atravesar (T).

/WebSEAL/sistema principal

Este subárbol contiene el espacio de la Web de un Policy Director WebSEAL Server determinado. Las siguientes consideraciones de seguridad se aplican a este objeto:

- Para acceder a cualquier otro objeto que se encuentre por debajo de este punto, deberá utilizar el permiso de atravesar (T).
- Si no se aplica ninguna otra ACL explícita, este objeto define (mediante valores heredados) la política de seguridad de todo el espacio de nombres de esta máquina.

/WebSEAL/sistema principal/archivo

Este subárbol es el objeto recurso que se comprueba para el acceso HTTP. Los permisos comprobados dependen de la operación solicitada.

Permisos WebSEAL

La siguiente tabla describe los permisos aplicables a la región WebSEAL del espacio de nombres:

Permisos del espacio de nombres de WebSEAL:	Acceso	Descripción
r	lectura	Visualizar el objeto HTTP
x	ejecutar	Ejecutar el programa CGI
d	eliminar	Eliminar el objeto HTTP
m	modificar	PUT de un objeto HTTP (Colocar - publicar - un objeto HTTP en el espacio de nombres WebSEAL)
l	listar	Generar una lista automática de directorios de HTTP
g	delegación	Asigna fiabilidad a un WebSEAL Server para que actúe en nombre de un cliente y pasa la petición a un WebSEAL Server conectado (junction)

Espacio de nombres NetSEAL

Las siguientes consideraciones sobre seguridad se aplican al objeto /NetSEAL:

- El objeto NetSEAL inicia la cadena de valores heredados de ACL para la región NetSEAL del espacio de nombres.
- Si no se aplica ninguna otra ACL explícita, este objeto define (mediante valores heredados) la política de seguridad de todos los servicios protegidos de NetSEAL en el espacio de nombres.
- Para acceder a este objeto y a cualquier otro que se encuentre por debajo de este punto, deberá utilizar el permiso de atravesar (T).

/NetSEAL/sistema principal

Este subárbol contiene todos los servicios protegidos de NetSEAL en una máquina servidor determinada. Las siguientes consideraciones de seguridad se aplican a este objeto:

- Para acceder a cualquier otro recurso que se encuentre por debajo de este punto, deberá utilizar el permiso de atravesar (T).
- Si no se aplica ninguna otra ACL explícita, este objeto define (mediante valores heredados) la política de seguridad de todos los servicios protegidos de NetSEAL en esta máquina.

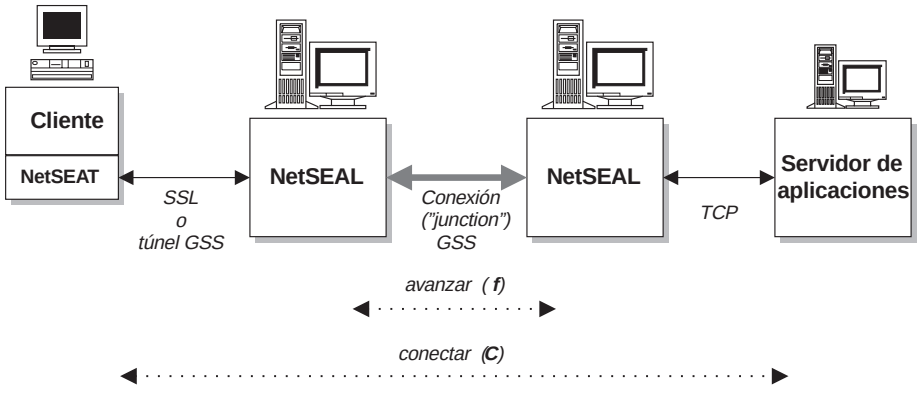
/NetSEAL/sistema principal/servicio

Este subárbol es el objeto que se comprueba para acceder al servicio protegido que representa. Los permisos comprobados dependen de la operación solicitada.

Permisos de NetSEAL

La siguiente tabla describe los permisos aplicables a la región NetSEAL del espacio de nombres:

Permisos sobre objetos protegidos de NetSEAL:	**Acceso**	**Descripción**
C	conexión	Conectarse con un NetSEAL
f	avanzar	Permitir una conexión de salida a través de una conexión (junction) NetSEAL; atravesar la conexión (junction).



Espacio de nombres Management

Las siguientes consideraciones sobre seguridad se aplican al objeto /Management:

- El objeto Management inicia la cadena de valores heredados de ACL para la región Management del espacio de nombres.

- Si no se aplica ninguna otra ACL explícita, este objeto define (mediante valores heredados) la política de seguridad de todo el espacio de nombres Management.
- Debe tener acceso al permiso de atravesar (T) para este objeto.

/Management/Server

El objeto contenedor /Management/server del espacio de nombres de objetos protegidos de Policy Director permite a los administradores efectuar tareas de gestión de servidor (cuando se han definido los permisos adecuados).

Utilice los controles de gestión para determinar si un usuario tiene permiso para crear, modificar o eliminar una definición de servidor. Las definiciones de servidor contienen información que permite a otros servidores de Policy Director, especialmente el Management Server (ivmgrd), localizar el servidor y comunicarse con él.

Se puede crear una definición de servidor para un Security Manager (secmgrd) o Authorization Server (ivacld) determinado como parte del proceso de instalación. Policy Director también elimina la definición que corresponde a un servidor cuando se desinstala dicho servidor.

La creación y eliminación de la definición se produce automáticamente; no es necesario que el administrador efectúe ningún paso especial para crear la definición. Sin embargo, el administrador debe tener permiso de modificación (m) sobre el objeto /Management/Server para poder crear la definición durante la instalación.

Además, el administrador debe tener permiso de eliminación (d) sobre el objeto /Management/Server para poder eliminar la definición durante la desinstalación.

Otras operaciones que pueden realizarse en una definición de servidor permiten que el usuario:

- Visualice las definiciones mediante el programa de utilidad **ivadmin**. Se puede otorgar al usuario el permiso de visualización (v) sobre el objeto servidor.
- Efectúe operaciones de gestión del servidor, como iniciar, detener, suspender, reanudar servidores o suprimir anotaciones cronológicas. El usuario debe tener permiso de administración de servidor (s) sobre el objeto servidor.
- Modifique partes de la definición utilizando el mandato **ivadmin server modify**. El usuario debe tener permiso de modificación (m) sobre el objeto servidor.

Permisos de gestión de servidor:	Acceso	Descripción
s	servidor	Efectúa operaciones de administración del servidor, como iniciar, detener, suspender, reanudar)
v	visualizar	Lista servidores
m	modificar	Crea una nueva definición de servidor
d	eliminar	Elimina una definición de servidor

/Management/ACL

Este objeto permite a los usuarios de administración efectuar tareas de alto nivel de gestión de ACL que pueden afectar a la política de seguridad del dominio seguro.

Permisos de gestión de ACL:	Acceso	Descripción

b	examinar	Visualiza el contenido del espacio de nombres que se encuentra bajo el objeto
a	unir	Une plantillas de ACL a objetos; elimina plantillas de ACL de objetos
m	modificar	Crea una nueva plantilla de ACL
d	eliminar	Elimina una plantilla de ACL existente. La ACL debe contener una entrada con el permiso de control (c) para este mismo usuario.
v	visualizar	Lista o visualiza una ACL

Debe definir administradores de ACL en el objeto de gestión de ACL por omisión. La entrada de ACL correspondiente al administrador puede contener cualquiera de los permisos indicados anteriormente. Estos permisos autorizan al administrador a crear nuevas plantillas de ACL, conectar ACL a objetos y eliminar plantillas de ACL.

Un administrador de ACL no puede modificar una ACL existente a menos que en dicha ACL haya una entrada para el administrador que contenga el permiso de control (c). Sólo el propietario de una ACL puede modificar sus entradas.

Recuerde que el creador de una nueva plantilla de ACL se convierte en la primera entrada de dicha ACL, con los permisos abcT que se establecen por omisión.

Por ejemplo, si `cell_admin` es una entrada en la ACL de gestión por omisión, con el permiso (m), cell_admin puede crear una nueva plantilla de ACL. El usuario cell_admin se convierte en la primera entrada de la nueva ACL, con los permisos abcT. El permiso de control (c) proporciona a cell_admin la propiedad de la ACL y permite a cell_admin modificar la ACL. A continuación, el usuario cell_admin podrá otorgar permisos de administración a otras entradas de usuarios de la ACL.

La propiedad de la ACL de gestión por omisión propiamente dicha se concede al usuario `cell-admin` y al grupo `iv-admin` por omisión.

/Management/action

Este objeto permite a los usuarios de administración efectuar tareas de gestión de ACL en un espacio de nombres de terceros. Las tareas de acción y los permisos asociados a las mismas son las siguientes:

Permisos de gestión de acciones (autorizaciones de terceros):	Acceso	Descripción
m	modificar	Crea una nueva acción
d	eliminar	Elimina una acción existente

Policy Director proporciona servicios de autorizaciones a las aplicaciones. Las aplicaciones que forman parte de la familia Policy Director incluyen WebSEAL (para aplicaciones de la Web) y NetSEAL (para aplicaciones basadas en TCP).

Las aplicaciones de terceros pueden efectuar llamadas a Policy Director Authorization Service a través de la API de autorizaciones de Policy Director. Para integrar una aplicación de terceros a Policy Director Authorization Service, son necesarios dos pasos:

- Definir el espacio de nombres de la aplicación.
- Aplicar permisos sobre objetos (recursos) que necesiten protección.

El administrador de un espacio de nombres de aplicación de terceros puede utilizar el programa de utilidad **ivadmin** para definir nuevos permisos y acciones. El administrador debe tener permisos de gestión y acciones para poder crear y eliminar dichos permisos y acciones.

/Management/réplica

El objeto contenedor /Management/Réplica del espacio de nombres de objetos protegidos de Policy Director controla la creación de réplicas de la base de datos de autorizaciones. Los controles de alto nivel sobre este objeto afectan a la operación del Management Server y los Security Managers del dominio seguro.

Los controles de gestión de réplicas se utilizan para determinar los procesos que pueden leer o actualizar la base de datos primaria de políticas de autorización para que la creación de réplicas se lleve a cabo correctamente.

Los controles y permisos asociados son los siguientes:

Permisos de gestión de réplicas:	Acceso	Descripción
v	visualizar	Leer la base de datos primaria de autorizaciones
m	modificar	Autorizar la modificación de la o las réplicas de bases de datos

Todos los servidores de Policy Director mantienen una réplica local de la base de datos de autorizaciones. Los servidores de Policy Director incluyen todos los Security Managers (secmgrd) y Authorization Servers (ivacld). Todos los servidores de Policy Director tienen permiso de visualización (v) sobre el objeto /Management/Replica.

El proceso de creación réplicas permite a estos procesos visualizar entradas y acceder a ellas fuera de la base de datos primaria de políticas de autorización. La instalación de Policy Director otorga automáticamente permiso de lectura (r) a cualquier servidor que requiera acceso a la base de datos de políticas de autorización.

Actualmente, Policy Director no utiliza el permiso de modificación (m). Actualmente, la base de datos primaria de políticas de autorización se modifica utilizando Management Console o el programa de utilidad **ivadmin**. Estas herramientas están sujetas a otras comprobaciones más precisas.

Directrices para tener un espacio de nombres seguro

Estas directrices proporcionan información que le ayudará a tener un espacio de nombres seguro:

- Defina una política de seguridad de alto nivel en los objetos contenedores del principio del espacio de nombres. Defina excepciones a esta política con una ACL explícita en objetos inferiores en la jerarquía.
- Organice el espacio de objetos protegidos para que la mayoría de objetos estén protegidos por ACL heredadas en vez de explícitas.

  Las ACL heredadas simplifican el mantenimiento del árbol porque reducen el número de ACL que deben mantenerse. Este mantenimiento inferior reduce el riesgo de un error que podría comprometer la red.
- Coloque los nuevos objetos en el árbol en el que heredarán los permisos adecuados.

Organice el árbol de objetos en un conjunto de subárboles en el que cada subárbol esté gobernado por una política de acceso específica. La política de acceso para todo un subárbol se determina definiendo una ACL explícita en la root del subárbol.

- Cree un conjunto de las plantillas de ACL esenciales y reutilícelas siempre que sea necesario.

  Como una plantilla de ACL es una definición de un solo origen, las modificaciones efectuadas en la plantilla afectarán a todos los objetos asociados a la ACL.
- Controle el acceso de usuarios mediante la utilización de grupos.

  Es posible que una ACL sólo esté formada por entradas de grupos. La adición o eliminación de usuarios de esos grupos puede controlar eficazmente el acceso a un objeto por usuarios individuales.

Plantillas de ACL de administración estándar

Las siguientes plantillas de ACL de administración por omisión son sugerencias de puntos de partida para asegurar regiones específicas del dominio seguro.

Se pueden añadir entradas para usuarios, grupos, autentificados por cualquiera y no autentificados. Estas entradas proporcionan un amplio ámbito de control y un mejor cumplimiento de los requisitos del espacio de objetos protegidos.

Anote todos los usuarios y grupos de cada ACL que tienen el permiso de control (c). Los usuarios, grupos (o ambos) que tienen el permiso de control *son los propietarios* de la ACL y pueden modificar las entradas de la ACL.

Root

Las entradas esenciales para la ACL del root por omisión (default-root) son las siguientes:

```
usuario cell_admin                      abcT
grupo iv-admin                          abcT
autentificado por cualquiera            T
no autentificado                        T
```

La ACL del root es muy básica. Cualquiera puede atravesar el espacio de nombres, pero no se puede ejecutar ninguna otra acción. Normalmente, no será necesario cambiar estas características. Sin embargo, la ACL del root tiene una función que resulta muy útil y que consiste en denegar rápidamente a un usuario individual o a un grupo de usuarios el acceso a todo el espacio de nombres.

Considere la siguiente entrada en la ACL del root:

```
usuario juan ----------------
```

La consecuencia de esta entrada (sin permisos) es que el `usuario juan` no podrá ni tan solo atravesar el objeto contenedor raíz (root). Este usuario no podrá acceder a todo el espacio de objetos protegidos, independientemente de los permisos que se le otorguen más abajo en el árbol.

Este enfoque también puede aplicarse a los espacios de objetos WebSEAL y NetSEAL. Por ejemplo, puede retirar el permiso de atravesar (T) a un usuario determinado de los objetos contenedores de /WebSEAL. Al retirar ese permiso, el

usuario no podrá entrar en absoluto al espacio de nombres de WebSEAL. El usuario no podrá entrar independientemente de los permisos que tenga sobre objetos dentro de estas regiones.

Espacio de objetos de WebSEAL

Las entradas más importantes de la ACL de WebSEAL (webseal por omisión) son las siguientes:

```
usuario cell_admin                  abcTdmlrx
grupo iv-admin                      abcTdmlrx
grupo servidores-webseal)           gTdmlrx
grupo servidores-ivmgrd             Tl
```

Durante la instalación, esta ACL por omisión se une al objeto contenedor de /WebSEAL en el espacio de nombres.

El grupo servidores-webseal contiene una entrada cada WebSEAL Server del dominio seguro. Los permisos por omisión permiten que los servidores respondan a peticiones del navegador.

El grupo servidores-ivmgrd contiene únicamente una entrada que representa a Management Server. La mayoría de peticiones de gestión efectuadas por Management Console se inician utilizando el Management Server para el WebSEAL Server de destino. Por lo tanto, el Management Server debe tener permiso para ejecutar la petición en el servidor de destino.

El permiso de atravesar permite la expansión del espacio de la Web tal como está representado en Management Console. El permiso de la lista permite a Management Console visualizar el contenido del espacio de la Web.

Espacio de objetos de NetSEAL

Las entradas más importantes de la ACL de NetSEAL (netseal por omisión) son las siguientes:

```
usuario cell_admin                  abcTC
grupo iv-admin                      abcTC
```

Durante la instalación, esta ACL se une al objeto contenedor de /NetSEAL en el espacio de nombres. Es necesario otorgar permiso de control (c) para acceder a un servicio protegido.

Espacio de objetos de Management

Las entradas más importantes de la ACL de Management (Management por omisión) son las siguientes:

```
usuario cell_admin                  abcTdmsv
grupo iv-admin                      abcTdmsv
grupo servidores-ivmgrd             Ts
autentificado por cualquiera        Tv
no autentificado                    Tv
```

Durante la instalación, esta ACL se une al objeto contenedor de /Management en el espacio de nombres.

Objeto de Replica Management (gestión de réplicas)

Las entradas más importantes de la ACL de Replica Management (replica por omisión) son las siguientes:

```
grupo secmgrd-servers                dmv
grupo ivacld-servers                 dmv
grupo servidores-ivmgrd              m
grupo iv-admin                       abcTv
usuario cell_admin                   abcTv
```

Evaluación de una ACL

Policy Director sigue un proceso de evaluación específico para determinar los permisos que otorga una ACL a un usuario determinado.

Evaluación de peticiones autentificadas

Policy Director evalúa un usuario autentificado en el siguiente orden:

1. Compara el ID de usuario con las entradas de usuario de la ACL. Los permisos otorgados son los de la entrada que coincida.

   ```
   Correcto: la evaluación se detiene aquí. Incorrecto: continuar con el
   siguiente paso.
   ```

2. Determina el grupo o grupos a los que pertenece el usuario y los compara con las entradas de grupo de la ACL.

   Si coincide más de una entrada de grupo, los permisos resultantes son una lógica “or” (más permisiva) de los permisos otorgados por cada entrada coincidente.

   ```
   Correcto: la evaluación se detiene aquí.
   Incorrecto: continuar con el siguiente paso.
   ```

3. Otorga los permisos de la entrada autentificada por cualquiera (si la hay).

   ```
   Correcto: la evaluación se detiene aquí.
   Incorrecto: continuar con el siguiente paso.
   ```

4. Existe una entidad implícita autentificada por cualquiera cuando no hay ninguna entrada de ACL autentificada por cualquiera. Esta entrada implícita no otorga permisos.

   ```
   Correcto: no se otorgan permisos.
   Fin del proceso de evaluación.
   ```

Evaluación de peticiones no autentificadas

Policy Director evalúa un usuario no autentificado otorgando los permisos desde la entrada no autentificada de la ACL.

La *entrada no autentificada* es una máscara (una operación “and” de bit) para la entrada autentificada por cualquiera cuando se determinan permisos. Únicamente se otorga un permiso para la entrada no autentificada si el permiso también aparece en la entrada autentificada por cualquiera.

Como la entrada no autentificada depende de la entrada autentificada por cualquiera, no tiene sentido que una ACL contenga una entrada no autentificada sin una entrada autentificada por cualquiera. Si una ACL contiene una entrada no autentificada sin ninguna entrada autentificada por cualquiera, la respuesta por omisión es no otorgar ningún permiso a la entrada no autentificada.

Ejemplos de entradas de ACL

Los permisos para usuarios o grupos (o ambos) específicos se definen indicando el tipo de entrada de ACL adecuado. En el siguiente ejemplo, el grupo documentación tiene privilegios de acceso completo:

```
grupo documentación --bcg--TdmsvC-lrx
```

Se puede restringir el acceso a otros usuarios no autentificados del dominio seguro (que no pertenezcan al grupo de documentación) utilizando la entrada de tipo autentificada por cualquiera.

```
autentificada por cualquiera -------T-------rx
```

Aún se puede limitar más el acceso a la entrada de tipo no autentificada para usuarios que no sean miembros del dominio seguro:

```
no autentificada -------T--------r-
```

Nota: Sin una entrada de ACL no autentificada, los usuarios no autentificados no podrán acceder a ningún documento seguro del dominio seguro de Policy Director.

Modelo de ACL breve para valores heredados de ACL

Para asegurar los recursos de red en un espacio de objetos protegidos, debe unirse una ACL a cada objeto.

Se puede asignar una ACL a un objeto de una de dos formas:

- Uniendo una ACL *explícita* al objeto.
- Permitiendo que el objeto *herede* su ACL de un objeto contenedor que le preceda en la jerarquía.

Si se adopta un esquema de ACL heredada se podrán reducir enormemente las tareas de administración de un dominio seguro. Esta sección trata de los conceptos de ACL heredadas o breves.

Visión general del modelo de ACL breve

Este principio es la base de la potencia de las operaciones con valores heredados de ACL: cualquier objeto que no tenga una ACL unida explícitamente hereda la ACL del objeto contenedor más próximo que tenga definida una ACL explícitamente. En otras palabras, todos objetos *sin* ACL unidas explícitamente heredan ACL de los objetos contenedores *con* ACL unidas explícitamente. Una cadena específica de valores heredados se rompe cuando se une una ACL explícita a un objeto.

Los valores heredados de ACL simplifican el trabajo de definir y mantener controles de acceso en un espacio de objetos grande y protegido. En un espacio de objetos normal, sólo será necesario unir unas pocas ACL a las ubicaciones clave para asegurar todo el espacio de objetos. En el modelo *breve* de ACL tan solo se unen unas pocas ACL a las ubicaciones clave.

Un espacio de nombres típico de Policy Director empieza por una sola ACL explícita que se une al objeto contenedor raíz (root). La ACL del root siempre debe existir y no ha de eliminarse nunca. Normalmente, se trata de una ACL con muy pocas limitaciones. Todos los objetos situados más abajo en el espacio de nombres heredarán esa ACL.

Cuando una región o subárbol de un espacio de nombres requiera unas limitaciones de control de accesos distintas, se unirá una ACL explícita al root de dicho subárbol. Esto interrumpirá la corriente de ACL heredadas procedentes del root del espacio de nombres primario que va al subárbol. A partir de la ACL explícita que acaba de crearse se iniciará una nueva cadena de valores heredados.

Plantilla de ACL del root por omisión

Policy Director comprueba los valores heredados empezando por el root del espacio de objetos protegidos. Si no define explícitamente una ACL en ningún otro objeto del árbol, todo el árbol heredará esta ACL del root.

Siempre hay una plantilla de ACL explícita definida en el root. Un administrador puede sustituir esta ACL por otra que contenga distintas entradas y otros valores de permisos. Pero la ACL del root nunca puede eliminarse completamente.

Policy Director define explícitamente la plantilla de la ACL del root durante la instalación y configuración iniciales de Policy Director, en la ventana Definición de ACL/Entrada de ACL:

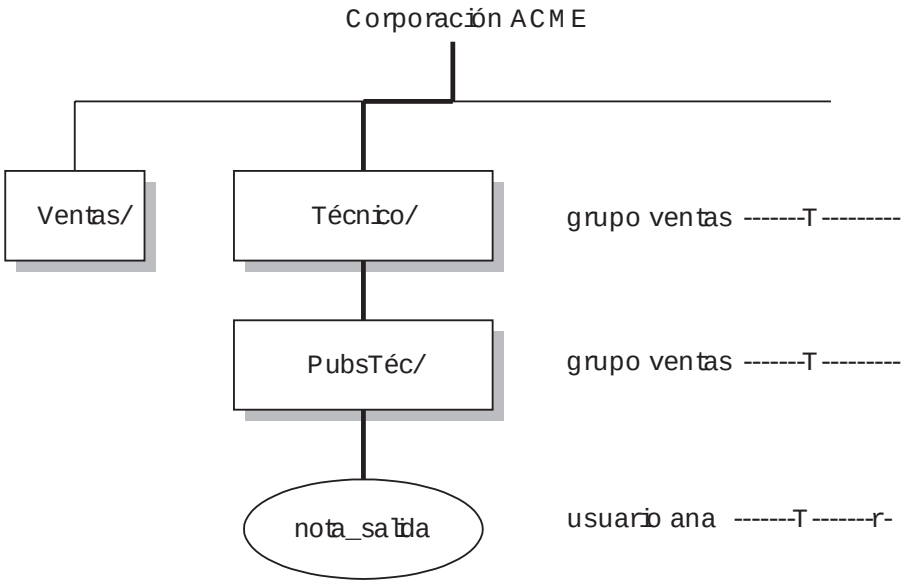
Nombre de ACL root por omisión
Descripción ACL del root por omisión

Permiso de atravesar

El permiso de atravesar (T) indica que la entidad identificada en la entrada de ACL tiene permiso para pasar a través del objeto. La entrada necesita permiso para pasar a través del objeto para tener acceso a un objeto que se encuentre más abajo en la jerarquía. El permiso de atravesar no otorga ningún otro permiso para el objeto. También debe proporcionar el permiso de atravesar para el objeto solicitado propiamente dicho.

La siguiente figura explica el funcionamiento del permiso de atravesar. Dentro de Corporación ACME hay un directorio Técnico que contiene también un subdirectorio PubsTéc. Lola (usuario lola) forma parte del departamento de Ventas y necesita poder acceder al directorio /Técnico/PubsTéc para revisar archivos de notas de salidas.

El administrador coloca una entrada de ACL de grupo ventas, con el permiso de atravesar (T) en los directorios /Técnico y /PubsTéc. Aunque el usuario lola no tiene otros permisos en estos dos directorios, puede pasar a través de ellos para acceder al archivo notas_salidas. Como este archivo tiene permisos de atravesar (T) y leer (r) para el usuario ana, podrá visualizar el archivo.



Se puede restringir fácilmente el acceso a una jerarquía que se encuentre bajo un objeto contenedor determinado, sin restablecer los permisos individuales sobre dichos objetos. Elimine simplemente el permiso de atravesar de la entrada de ACL adecuada. Al eliminar el permiso de atravesar de un objeto de directorio se protegen todos los objetos que están más abajo en la jerarquía, incluso si esos objetos contienen otras ACL menos restrictivas.

Por ejemplo, el grupo de ventas debe tener el permiso de atravesar (T) en el directorio Técnico. Si el grupo ventas no lo tuviese, Lola no podría acceder al archivos notas_salidas aunque tuviese el permiso de lectura (r) sobre el archivo.

Resolución de una petición de acceso

La operación de herencia empieza con la ACL del root y afecta a todos los objetos del espacio de nombres hasta que llega a un objeto que tiene una ACL explícita. Al llegar a este punto se inicia una nueva cadena de valores heredados.

Los objetos que se encuentran bajo una ACL definida explícitamente heredan los nuevos controles de acceso. Si se suprime una ACL explícita, el control de accesos de todos los objetos retorna al directorio u objeto contenedor que tenga una ACL definida explícitamente.

Cuando un usuario intenta acceder a un objeto seguro, Policy Director comprueba si el usuario tiene los permisos necesarios para acceder al objeto. Por ejemplo, un objeto seguro podría ser un documento Web. Efectúa la comprobación buscando en todos los objetos de la jerarquía los permisos adecuados heredados o definidos explícitamente.

Se puede denegar el acceso de un usuario a un objeto. Policy Director deniega el acceso cuando algún objeto de directorio u objeto contenedor de la jerarquía superior no incluye el permiso de atravesar (T) para el usuario. Policy Director también deniega el acceso cuando el objeto de destino no contiene permisos suficientes para realizar la operación solicitada.

Para que una comprobación de acceso sea correcta, el solicitante debe tener estos dos elementos:

1. Permiso para atravesar la vía de acceso hasta el objeto solicitado.
2. Permisos adecuados sobre el objeto solicitado.

El siguiente ejemplo ilustra el proceso en el que se decide si un usuario puede leer (visualizar) un objeto:

```
/acme/técnico/proyecto_Y/actual/informe.html
```

Policy Director comprueba si hay lo lo siguiente:

1. Permiso de atravesar en la ACL del root definida explícitamente (/).
2. Permiso de atravesar en cualquier ACL explícita conectada a los directorios:acme, técnico, proyecto_Y u actual.
3. Permiso de lectura para el archivo propiamente dicho (informe.html).

Policy Director deniega el acceso del usuario cuando el usuario no pasa la comprobación de acceso en cualquiera de estos puntos a lo largo de toda la jerarquía del objeto.

Plantillas de ACL aplicadas a distintos tipos de objetos

Se pueden definir permisos para varias operaciones en una plantilla de ACL. Puede que tan solo un subconjunto de estas posibles operaciones se aplique a un objeto determinado al que esté unida la ACL.

El motivo de este comportamiento está relacionado con las dos características de Policy Director destinadas a facilitar la administración:

- Plantillas de ACL
- Valores heredados de ACL

Las plantillas de ACL permiten unir una misma definición de ACL a varios objetos del espacio de nombres de objetos protegidos. La definición de ACL tiene suficientes entradas para cumplir con las necesidades de todos los objetos a los que se aplicará la ACL. No obstante, tan solo algunas de las entradas afectarán a cada uno de los objetos.

En el modelo de valores heredados de ACL, todos los objetos que no lleven unida una ACL explícita heredarán las definiciones de políticas. Estas definiciones de políticas heredadas proceden de la ACL más próxima aplicada a un objeto que la preceda en la jerarquía.

En resumen, una plantilla de ACL debe describir todos los permisos necesarios para todos los tipos de objetos a los que va a aplicarse. Las plantillas de ACL no solo describen el objeto al que están unidas.

Ejemplo de valores heredados de ACL

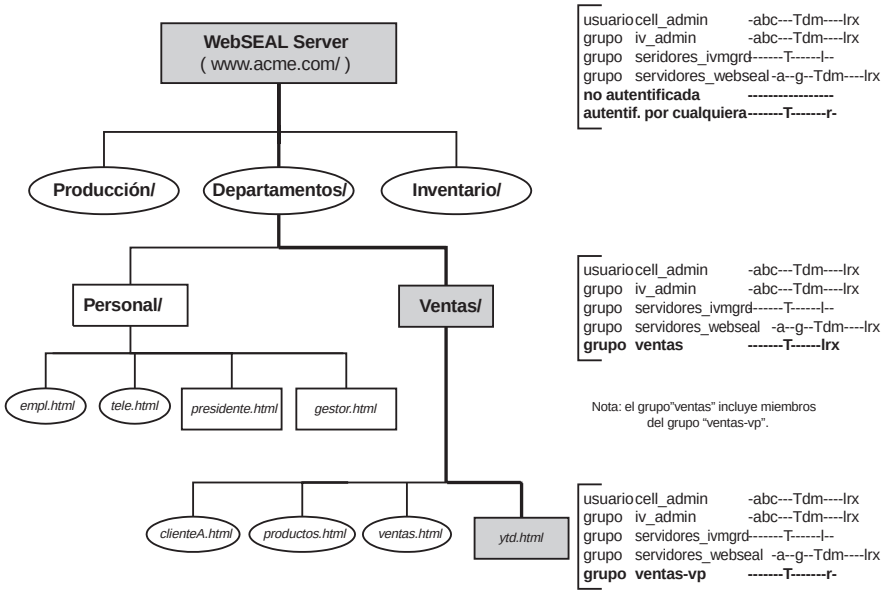
La siguiente figura ilustra el impacto de una combinación de ACL explícitas y heredadas en el espacio de nombres de una empresa.

Un espacio de objetos de una empresa tiene definida una política de seguridad en el objeto root. El root va seguido del objeto contenedor /WebSEAL y de subárboles de departamentos controlados individualmente.

En este ejemplo, el grupo venta es el propietario del subárbol de departamento. Tenga en cuenta que la ACL de este subárbol ya no reconoce las entradas de tipo no autentificada o autentificada por cualquiera. El archivo de ventas Año Hasta Fecha (ahf.html) tiene una ACL explícita. Esta ACL explícita otorga el permiso de

lectura (r) a los miembros del grupo ventas-vp. Los miembros del grupo ventas-vp también son miembros del grupo ventas).

Nota: No es necesario cambiar este esquema de ACL añadiendo o eliminando usuarios del dominio seguro. Los nuevos usuarios se añaden simplemente al grupo o grupos adecuados. Del mismo modo, puede eliminarse usuarios de estos grupos.



Delegación de la gestión de ACL

La distribución de responsabilidades de administración en un dominio seguro se conoce como delegación de gestiones. La necesidad de una delegación de gestiones aparece generalmente cuando crece la demanda en un lugar grande que contenga varias divisiones distintas de departamentos o recursos.

Normalmente, un espacio de objetos grande puede organizarse en regiones que representen esos departamentos o divisiones. De este modo, las distintas regiones del dominio pueden organizarse mejor. El mantenimiento de cada región puede realizarlo un administrador que esté más familiarizado con las salidas y posibilidades de esa rama.

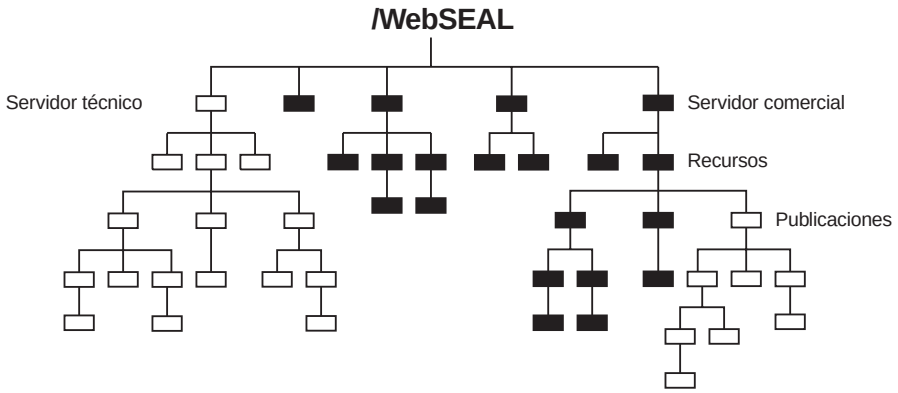
De este modo, las distintas regiones del dominio podrán organizarse mejor. El administrador, que está más familiarizado con la problematica y las necesidades de esa rama, efectúa el mantenimiento de cada región.

En un dominio seguro de Policy Director, la cuenta cell_admin es inicialmente la única cuenta con permiso de administración. Como administrador de célula (cell_admin), puede crear cuentas de gestión y asignarles controles adecuados que correspondan a las distintas regiones del espacio de objetos.

Estructuración del espacio de nombres para la delegación de gestiones

Estructure el espacio de objetos para que contenga distintas regiones o ramas en las que pueden llevarse a cabo las operaciones de subadministración específicas de cada rama.

En el ejemplo que sigue, las regiones Técnico y Publicaciones del espacio de objetos requieren un control de gestión separado. El control de esas regiones empieza en el root de cada región y se extiende a todos los objetos que le siguen.



Espacio de la web

Utilización de usuarios y grupos administrativos por omisión

Policy Director crea varios grupos administrativos importantes. Por omisión, se otorga a dichos usuarios o grupos (o a ambos) permisos especiales para controlar y gestionar todas las operaciones en el dominio seguro. Esta política de seguridad por omisión se define mediante las ACL creadas durante la instalación.

Las siguientes secciones detallan las funciones específicas asignadas a cada usuario y grupo durante la instalación. El administrador puede personalizar estos privilegios posteriormente para acomodar las cambiantes políticas de gestión.

usuario cell_admin

Este usuario representa al administrador del dominio seguro al que se han otorgado derechos completos para todas las operaciones del dominio seguro.

Esta política puede cambiarse a medida que el espacio de objetos crezca. La política se cambia delegando permisos de gestión a otros usuarios. Es posible que la política también pueda cambiarse revocando determinados permisos (o todos) de cell_admin.

grupo iv-admin

Este grupo representa al grupo del administrador. Como cell_admin, todos los miembros de este grupo son considerados administradores del dominio seguro por la política por omisión. Todas las ACL por omisión otorgan exactamente los mismos permisos al usuario cell_admin y al grupo iv-admin.

Se puede dar fácilmente una función administrativa a los usuarios añadiéndoles al grupo iv-admin. Recuerde que este procedimiento puede causar problemas. Cuando un usuario se convierta en miembro de ese grupo, tendrá las ACL por omisión. Con las ACL por omisión, el usuario tendrá todos los derechos para hacer lo que quiera en cualquier objeto de todo el espacio de nombres.

La política por omisión de este grupo puede cambiarse. La política por omisión puede cambiarse, por ejemplo, delegando los permisos de gestión a otros usuarios. La política por omisión también puede cambiarse revocando de iv-admin algunos de los permisos de gestión (o todos).

grupo ivmgrd-servers

Este grupo contiene el Management Server. Actualmente, Policy Director requiere que exista exactamente un Management Server en el dominio seguro. Por lo tanto, este grupo contendrá únicamente esta entrada.

La mayoría de peticiones de gestión efectuadas por la consola se ejecutan utilizando el Management Server para el Policy Director Server de destino. Debido a este proceso, el Management Server debe tener autorización para realizar la petición en el servidor de destino. Por este motivo, se concede a este grupo el permiso de administración de servidor (s) en la ACL de gestión por omisión, y el permiso de lista (l) en todo el espacio de la Web.

grupo webseal-servers

Este grupo contiene todos los WebSEAL Servers del dominio seguro. La ACL de WebSEAL por omisión otorga a estos servidores todo el conjunto de permisos específico de HTTP así como el permiso de delegación. Esta política permite a todos los WebSEAL Servers conectarse (junction) con todos los demás WebSEAL Servers. Una modificación de esta política podría otorgar estas políticas en una base servidor a servidor.

Creación de usuarios de administración

Con Policy Director, podrá crear cuentas de administración con distintos grados de responsabilidad. La responsabilidad se delega a los administradores a través de la colocación estratégica de las ACL de administración. La siguiente lista ilustra posibles funciones de administración:

Responsabilidades de administración de ACL

El administrador de ACL puede controlar parte o toda una región del espacio de nombres de objetos protegidos, dependiendo de dónde se coloque la ACL de administración. La entrada de ACL del administrador podría contener los permisos b, a y T, más cualquier otro permiso que fuese adecuado para operaciones sobre objetos de esa región.

El administrador puede utilizar Management Console para unir las ACL a objetos del espacio de nombres indicado. El administrador puede utilizar el conjunto existente de plantillas de ACL. Las ACL se unen utilizando el permiso de unión (a). Este administrador no tiene permisos para crear, cambiar o eliminar plantillas de ACL.

Responsabilidades de políticas de ACL

El administrador de políticas de ACL debe responsabilizarse de controlar la creación y modificación de todas las plantillas de ACL utilizadas en el dominio seguro. Al administrador de políticas de ACL deberían otorgársele los permisos d, b, m y v en el objeto /Management o /Management/ACL.

Este administrador de políticas de ACL podrá crear nuevas plantillas de ACL utilizando el permiso (m). Como creador de una nueva plantilla, el administrador pasa a ser, por omisión, la primera entrada de la nueva plantilla de ACL con los permisos abcT. El permiso de control (c) proporciona efectivamente al administrador la propiedad de la ACL y, por lo tanto, la posibilidad de cambiar dicha ACL.

Como propietario de la ACL, el administrador puede utilizar el permiso de eliminación (d) que se otorga en la ACL de gestión. El administrador utiliza este permiso para eliminar la ACL de la lista de plantillas. Tan solo el propietario de una plantilla de ACL puede eliminarla.

Responsabilidades de gestión del servidor
El administrador tiene los permisos d, m, s y v sobre el objeto /Management/Server. Este administrador puede realizar operaciones que impliquen los servidores de Policy Director.

Responsabilidades de acciones de autorización
Este administrador tiene los permisos (d) y (m) sobre el objeto /Management/Action. El administrador podrá crear o eliminar todos los permisos creados para aplicaciones de terceros.

En el apartado “Espacio de nombres Management” en la página 93 encontrará más información sobre la gestión del espacio de nombres.

Ejemplo de plantilla de ACL de administración

El siguiente ejemplo explica cómo consigue un usuario derechos de administración.

- La siguiente ACL de /WebSEAL proporciona derechos de administración a usuario ana:

```
usuario cell_admin              abcTdmlrx
grupo iv-admin                  abcTdmlrx
grupo servidores-webseal)       gTdmlrx
grupo servidores-ivmgrd         Tl
usuario ana                     abcTdmlrx
autentificado por cualquiera    Trx
no autentificado                Trx
```

- La siguiente ACL de /NetSEAL proporciona derechos de administración a usuario ana:

```
usuario cell_admin                  abcTC
grupo iv-admin                      abcTC
usuario ana                         abcTC
autentificado por cualquiera        TC
no autentificado                    TC
```

Ejemplo de delegación de gestión

Un espacio de objetos grande puede requerir que muchos usuarios de administración gestionen varias subramas. En este supuesto, las ACL para los directorios que se encuentren en la vía de acceso a cada una de esas ramas deben contener entradas para cada cuenta con permiso para atravesar. En un lugar que tenga muchos usuarios de administración, estas ACL pueden contener una larga lista de entradas que representen a todas estas cuentas de administración.

La siguiente técnica resuelve el problema de tener numerosas entradas de ACL para administradores:

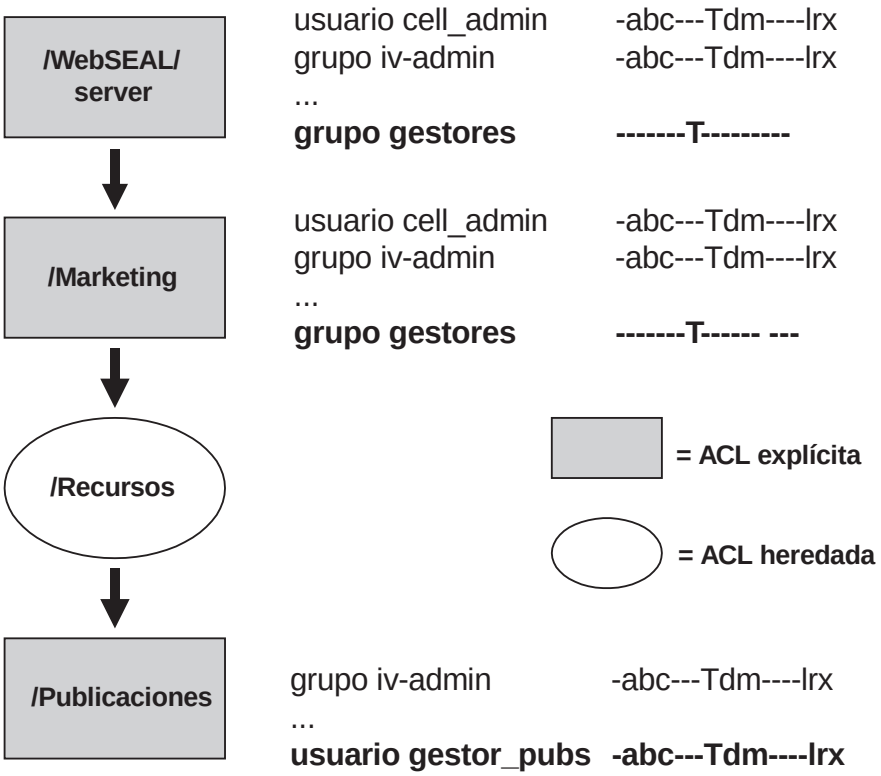
1. Cree una cuenta de grupo de administración.
2. Añada todos los nuevos usuarios de administración a ese grupo.
3. Añada este grupo como entrada de ACL (con permiso de atravesar) a los directorios que lleven a cada subrama y que requieran una delegación de la gestión.

4. Añada a cada ACL del root de la rama la entrada de usuario de administración pertinente (con b, c, T, y demás permisos adecuados).
5. El administrador podrá eliminar entonces del root la entrada de ACL de grupo de administración (y cualquier otra entrada que desee).

   Ahora, tan solo el usuario tendrá control sobre el root y todos los objetos que estén por debajo de él.

En el ejemplo que sigue, el grupo gestores se ha creado para que contenga todos los usuarios de administración. El usuario gestor_pubs es miembro de ese grupo y, por lo tanto, tiene el permiso de atravesar necesario para navegar hasta el directorio Publicaciones.

El directorio Publicaciones incluye la entrada usuario gestor-pubs en su ACL. El gestor-pubs es el administrador delegado de esta rama y tiene los permisos adecuados. Como administrador delegado, gestor-pubs puede eliminar la cuenta del grupo gestores (y otras entradas de ACL que desee) de la ACL Publicaciones. Eliminando la cuenta del grupo y las demás entradas de la ACL, el administrador delegado adquirirá el control total de esa rama del espacio de la Web.



Capítulo 8. Aplicación del control de acceso

En un dominio seguro, los recursos pueden protegerse mediante la utilización de plantillas de políticas. Las plantillas de políticas contienen permisos que controlan la utilización de un recurso. Las plantillas de políticas deben unirse a la representación del objeto de espacio de nombres del recurso que requiere protección.

Policy Director reconoce y utiliza un tipo de plantilla de política llamado ACL. Las ACL se utilizan para estampar la política de seguridad de una empresa en los recursos que pertenecen al dominio seguro.

Este capítulo habla de las tareas comunes necesarias para gestionar el espacio de objetos y aplicar el control de acceso.

Este capítulo incluye los siguientes temas:

Visión general de la gestión de ACL

El panel de tareas de gestión de ACL de Management Console se utiliza para crear, modificar y eliminar entradas de ACL.

1. Inicie la sesión con Management Console como administrador de gestión de ACL, por ejemplo `cell_admin`.
2. Pulse el botón en el separador de tarea **ACL**.

   Aparecerá el panel de tarea de gestión ACL.

Botones de acción de tareas de gestión de ACL

Los botones de acción de **ACL** se utilizan para realizar operaciones de gestión de ACL. La siguiente tabla describe las tareas que realiza cada botón de acción:

Botón de acción	Descripción
Nueva ACL	Crea una nueva plantilla de ACL.
Nueva entrada	Añade una nueva entrada a la plantilla de ACL seleccionada.
Guardar	Guarda esta plantilla de ACL. La ACL aparece en la vista de lista Nombre de ACL.
Eliminar	Elimina la plantilla de ACL seleccionada.
Obtener	Recupera información sobre una plantilla de ACL indicada específicamente y rellena la vista de detalles de ACL. Especifique la ACL en el campo Nombre de ACL de la sección Definición de ACL.
Lista	Renueva la vista de lista.
Dónde se usa	Visualiza la lista completa de objetos protegidos a la que está unida la plantilla de ACL seleccionada. Esta visualización aparece en la sección Tablón de anuncios de Console.

Tareas de gestión de ACL

Pueden realizarse las siguientes operaciones de gestión de ACL:

- Crear una nueva plantilla de ACL.
- Añadir una entrada de ACL.
- Editar permisos para una entrada de ACL.
- Eliminar una plantilla de ACL.

Creación de una nueva plantilla de ACL

Para crear una nueva plantilla de ACL, se puede empezar con una de las plantillas de ACL por omisión y modificarla para que contenga las especificaciones que desee el usuario.

1. En la lista **Nombre de ACL**, arrastre el icono de la plantilla de ACL por omisión que desee utilizar. Después, la plantilla podrá utilizarse en el Tablón de anuncios como base de la nueva ACL.
2. En los botones de acción de ACL, pulse en **Nueva ACL**.

   La información anterior del área de Definición de ACL se borrará y los campos quedarán preparados para nuevas entradas.

   Por omisión, la identidad con la que se ha efectuado el inicio de sesión se convierte en la primera entrada de ACL, con los permisos abcT. El permiso de control (c) proporciona autorizaciones de propietario para esta ACL.
3. Escriba el nombre de la ACL en el campo **Nombre de ACL**.
4. Con el tabulador, vaya al campo **Descripción** y escriba una frase que describa la finalidad de la ACL (cómo o por qué va a aplicarse).
5. Arrastre el icono **ACL** por omisión del tablón de anuncios al área Entrada de ACL de la nueva Definición de ACL.

   La nueva ACL contiene ahora las entradas de la ACL por omisión.
6. Efectúe las modificaciones adecuadas en las entradas.
7. Pulse el botón **Guardar**.

Adición de una entrada de ACL

Para añadir una entrada de ACL:

1. En la lista **Nombre de ACL**, seleccione una plantilla de ACL.
2. Pulse el botón del ratón en el botón de acción **Nueva entrada**.

   El área Entrada de ACL se borrará y restablecerá para quedar preparada para una nueva entrada.
3. Pulse el botón del ratón y manténgalo pulsado en el campo **Tipo**.

   Aparecerá un menú desplegable.
4. Seleccione el tipo usuario, grupo, no autentificado o autentificado por cualquiera.
5. Pulse en botón en el campo **ID** y escriba el ID correcto.

   También puede arrastrar y soltar los iconos de usuario y grupo desde la vista **Gestión de cuentas**. Pulse el botón en el separador de tarea **Cuentas** y coloque la vista **Gestión de cuentas** en el área del panel inferior de Console.
6. Utilice los recuadros de selección de los permisos para aplicar los permisos pertinentes a esta entrada.
7. Pulse el botón **Guardar** para confirmar la entrada en la ACL.

Edición de permisos para una entrada de ACL

Para editar permisos para una entrada de ACL:

1. En el área de Definición de ACL, seleccione la entrada.
2. En el área de Entrada de ACL, elija los permisos adecuados seleccionando o no los recuadros de selección de los permisos.
3. Pulse el botón **Guardar** para confirmar los cambios.

Eliminación de una plantilla de ACL

Para eliminar una plantilla de ACL:

1. En la lista **Nombre de ACL**, seleccione la plantilla de ACL que desea eliminar.
2. Pulse el botón del ratón en el botón **Eliminar**.

   Aparecerá un recuadro de aviso.
3. Pulse el botón **Continuar**.

   Management Console no suprimirá una ACL que siga estando unida a un objeto. En la barra de estado aparecerá un mensaje indicando esta situación.

Ejemplo:

Ha unido una ACL destinada a miembros del grupo `webtest`. El grupo `webtest` es el grupo que está desarrollando y probando nuevas páginas HTML. Después de efectuar la prueba, podrá eliminar esta ACL explícita para que otros miembros el dominio seguro puedan disponer de ella.

Ejemplo de procedimiento para crear una nueva plantilla de ACL

Para crear una nueva plantilla de ACL:

1. Pulse el botón del ratón en el botón de acción **Nuevo**.

   La información anterior del área de Definición de ACL se borrará y los campos quedarán preparados para nuevas entradas.

   Por omisión, la identidad con la que se ha efectuado el inicio de sesión se convierte en la primera entrada de ACL, con los permisos abcT.
2. Escriba el nombre de la ACL en el campo **Nombre de ACL**.
3. Con el tabulador, vaya al campo **Descripción** y escriba una frase que describa la finalidad de la ACL (cómo o por qué va a aplicarse).
4. Pulse el botón **Guardar** para confirmar esta nueva ACL en la Lista de ACL.
5. Pulse el botón del ratón en el botón **Nueva entrada**.

   El área Entrada de ACL se borrará y restablecerá para quedar preparada para una nueva entrada.
6. Pulse el botón del ratón y manténgalo pulsado en el campo **Tipo**.

   Aparecerá un menú desplegable.
7. Pulse el botón en **no autentificado** y no otorgue ningún permiso.
8. Pulse el botón **Guardar**.

   La entrada aparecerá en el área Definición de ACL.
9. Ejecute los mismos procedimientos para añadir una entrada autentificada por cualquiera que no tenga ningún permiso.
10. Pulse el botón en el separador de tarea **Cuentas**.

    El panel Gestión de cuentas aparecerá como panel superior.
11. Pulse el botón del ratón en el botón **Colocar tarea abajo** para colocar el panel de Gestión de cuentas en la parte inferior de Console.

12. Para crear una nueva entrada de grupo, pulse el botón en **Nueva entrada** (panel ACL).
13. En la lista **Grupos** del panel Cuentas, arrastre y suelte un icono de **grupo** al campo **ID** del área Entrada de ACL.

    Los campos **Tipo** e **ID** se rellenarán con la información adecuada.
14. Compruebe si hay los permisos adecuados.
15. Pulse el botón **Guardar** para confirmar esta entrada en la ACL.

Visión general de la gestión del espacio de objetos

El panel de la tarea de gestión Espacio de objetos de Management Console se utiliza para unir las ACL a objetos y eliminar las ACL de los objetos.

1. Inicie la sesión con Management Console como usuario con permisos de gestión de ACL, como `cell_admin`.
2. Pulse el botón en el separador de tarea **Espacio de objetos**.

   Aparecerá el panel de la tarea de gestión Espacio de objetos.

Botones de acción para tareas de gestión del espacio de objetos

Los botones de acción del **Espacio de objetos** se utilizan para realizar operaciones de gestión del espacio de objetos. La siguiente tabla describe las tareas que realiza cada botón de acción:

Botón de acción	Descripción
Unir ACL	Asigna una ACL a un objeto.
Eliminar ACL	Elimina una ACL de un objeto.
Buscar ACL	Busca todos los objetos marcados explícitamente con una ACL específica. Los objetos están listados en el panel inferior de Console.
Guardar ACL	Permite guardar una modificación efectuada en una ACL mientras se utilizaba la vista Editar ACL.
Lista	Renueva el árbol del espacio de objetos.

Tareas de gestión del Espacio de objetos

Se pueden realizar las siguientes operaciones de gestión del espacio de objetos:

- Unir una ACL a un objeto.
- Suprimir una ACL explícita de un objeto.

Unión de una ACL a un objeto

Para unir y eliminar las ACL debe tener los permisos de gestión pertinentes. En particular, debe tener el permiso de unión (a) para aplicar una ACL a objetos y eliminar la ACL de los objetos.

1. Coloque el panel de tarea de gestión ACL en la sección inferior de Console.
2. Pulse el botón en el panel Espacio de objetos del panel superior de Console.
3. Amplíe la región adecuada del árbol de Espacio de objetos y seleccione el objeto de destino al que debe unirse una ACL explícita.
4. Arrastre el icono de la plantilla de ACL adecuada desde la lista **Nombre de ACL** y suéltela en el objeto seleccionado del árbol del Espacio de objetos.

Eliminación de una ACL explícita de un objeto

Para unir y eliminar las ACL debe tener los permisos de gestión pertinentes. En particular, debe tener el permiso de unión (a) para aplicar una ACL a objetos y eliminar la ACL de los objetos.

1. Pulse el botón en el separador de tarea **Espacio de objetos**.
2. Amplíe la región adecuada del árbol de Espacio de objetos y seleccione el objeto de destino que tiene unida la ACL explícita.
3. Pulse el botón del ratón en el botón **Eliminar ACL**.

Capítulo 9. Gestión de usuarios proxy

Uno de los conjuntos de productos de seguridad de IBM SecureWay FirstSecure (FirstSecure) es IBM SecureWay Boundary Server para Windows NT y AIX (Boundary Server). Si LDAP es su registro de usuarios por omisión, puede utilizar Policy Director junto con Boundary Server para conseguir una solución integrada de usuario proxy de IBM Firewall y Policy Director.

La información más actualizada sobre FirstSecure y sus componentes se encuentra en el sitio Web:

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

Presentación de la seguridad de límites

Del mismo modo que Policy Director, Boundary Server es uno de los componentes proporcionados con el paquete de seguridad del producto IBM SecureWay FirstSecure. Boundary Server o Policy Director también se pueden comprar por separado y utilizarlos como productos autónomos—sin necesidad de comprar todo el paquete FirstSecure.

La seguridad de límites no sólo protege la red, las aplicaciones y la información, sino que también amplía su alcance. Una seguridad de límites adecuada requiere que se controle quién puede acceder a la red y qué información entra y sale de la red. Boundary Server proporciona protección de cortafuego, seguridad de contenidos y VPN. Boundary Server crea un límite con Internet que puede utilizarse para bloquear potencialmente peligrosos virus, script de Java, applets, controles ActiveX e incluso e-mail basura (SPAM).

En el manual *IBM SecureWay Boundary Server Up and Running* que se facilita con el producto IBM SecureWay Boundary Server encontrará información para planificar, instalar, configurar y utilizar Boundary Server, así como para resolver problemas.

Boundary Server es un paquete de productos. Boundary Server reúne lo mejor de la tecnología de seguridad para lograr una solución integrada. Esta solución incluye el soporte y los servicios de IBM, que pueden comprarse por separado.

Uno de los componentes de Boundary Server es IBM SecureWay Firewall Versión 4.1 (Firewall).

Integración con IBM Firewall

La finalidad de un *cortafuego* es evitar en la red la entrada o salida de comunicaciones no deseadas o no autorizadas. Un cortafuego sirve como bloqueo entre una o más redes privadas internas seguras y otras redes (no seguras) de la Internet pública.

IBM Firewall es un programa de seguridad de la red. IBM SecureWay Firewall Versión 4.1 incluye las siguientes características:

- Mejoras proxy para seguridad en el correo
- Socks Protocol, Versión 5, mejoras
- Remote Access Service (RAS)

- HTTP proxy

HTTP proxy maneja las peticiones del navegador a través de SecureWay Firewall, que elimina la necesidad de servidores Socks para la navegación por la Web. Los usuarios pueden acceder a información útil de Internet sin comprometer la seguridad de sus redes internas y sin que sea necesario que los entornos de sus clientes implementen HTTP proxy.

Para poder instalar SecureWay Firewall, debe asegurarse de que tiene instalados y configurados los requisitos previos necesarios. También debe definir interfaces seguras, determinar y configurar la política de seguridad y definir objetos de la red. Deben definirse los siguientes objetos clave de red:

- Interfaces seguras en el cortafuego.
- Interfaces inseguras en el cortafuego.
- Una red asegurada.
- Cada subred en la red asegurada.
- Un objeto de red del sistema principal para los servidores Security Dynamics y los servidores del dominio Windows NT, si corresponde.

En el manual *IBM SecureWay Boundary Server Up and Running* que se facilita con Boundary Server encontrará información completa sobre la instalación y configuración.

Descripción de tipos de usuarios

Los administradores de IBM Firewall son los responsables de configurar, crear y modificar las definiciones de usuarios proxy, pero no podrán crear ni modificar definiciones de otros administradores del cortafuego.

Los administradores de Firewall realizan las siguientes tareas administrativas:

- Añadir usuarios a IBM Firewall para que puedan acceder a sistemas principales fuera de su propia red protegida.
- Modificar los atributos de los usuarios que acceden al cortafuego.
- Eliminar usuarios que ya no necesiten tener acceso fuera de su propia red.

En una solución integrada de IBM Firewall y Policy Director, es el administrador de Policy Director quien se hace cargo de la gestión de usuarios proxy.

Usuarios de Firewall

Los usuarios de la red asegurada pueden acceder a una red que no sea segura utilizando un mecanismo de red (como Socks o proxy). Si desea permitir que los usuarios asegurados utilicen una red que no sea segura (proxy), deberá configurar y definir unas conexiones adecuadas que permitan ese tipo de tráfico.

Los servicios que se lleven a cabo dependen de las decisiones que haya tomado en la etapa de planificación. La entrada en vigor de un servicio requiere a menudo la conexión de configuraciones que permitan determinados tipos de tráfico. Por ejemplo, si desea permitir que los usuarios asegurados naveguen por la Web en Internet utilizando HTTP Proxy, no sólo deberá configurar el daemon HTTP Proxy en el cortafuego (Firewall), sino que también deberá definir conexiones que permitan el tráfico HTTP.

Si va a necesitar la autentificación para funciones como, por ejemplo, el acceso de salida a la Web, defina estos usuarios para IBM Firewall.

Usuarios proxy

La administración de Policy Director puede configurarse para gestionar usuarios proxy como si fuesen una extensión de usuarios de Policy Director. Para conseguir una solución integrada de Policy Director e IBM Firewall, el administrador de Policy Director debe configurar a los usuarios como usuarios proxy de Policy Director.

Un usuario proxy es alguien que utiliza servicios cortafuego, como el servicio HTTP proxy, para acceder a sitios Web de Internet desde dentro de una red de empresa. Los usuarios proxy pueden utilizar servicios a través del cortafuego pero no tienen acceso a la máquina cortafuego y no pueden iniciar sesiones con la máquina cortafuego.

Habilitación de la gestión de usuarios proxy

Para poder llevar a cabo la gestión de usuarios proxy, debe habilitar esta característica en Management Console. Para habilitar las funciones de Proxy User, debe editar el archivo console.properties.

Encontrará el archivo console.properties en:

Windows: `C:\Archivos de programa\IBM\IVConsole\console.properties`

UNIX: `/opt/intraverse/ivconsole/console.properties`

Para configurar la gestión de usuarios proxy:

1. Utilizando un editor de texto, abra el archivo console.properties.
2. Suprima el símbolo de comentario (#) del principio de esta línea:
   ```
   #6, ProxyUsersTaskView              = IV.ProxyUserTask.ProxyUsersTaskView
   ```
3. Reinicie Management Console para habilitar la característica de gestión de Usuario proxy .

Presentación de la gestión de usuarios proxy

En Policy Director, los usuarios del cortafuego (Firewall) se denominan *usuarios proxy*. Policy Director Management Console permite gestionar usuarios proxy.

Los administradores de Policy Director realizan las siguientes tareas administrativas:

- Añadir usuarios como usuario proxy para que puedan utilizar los servicios del cortafuego.
- Modificar los atributos de los usuarios proxy que utilicen los servicios del cortafuego.
- Eliminar usuarios proxy que ya no necesiten utilizar servicios de cortafuego.

Los administradores de Firewall (cortafuego) deberían consultar la documentación de BM Firewall donde encontrarán más información sobre la forma de llevar a cabo estas tareas administrativas.

Utilización del panel de gestión de usuarios proxy

El panel de la tarea de gestión Usuarios contiene una vista de árbol **Usuarios** y una vista de detalles **Usuario proxy**.

Utilización de botones de acción para tareas de gestión de usuarios proxy

Los botones de acción de **Usuario proxy** se utilizan para realizar operaciones de gestión de usuarios proxy. La siguiente tabla describe las tareas que realiza cada botón de acción:

Botón de acción	Descripción
Guardar	Crea un nuevo usuario proxy si se ha seleccionado un usuario de Policy Director en la vista de árbol de usuarios. O cambia un usuario proxy existente si se ha seleccionado un usuario proxy existente en la vista de árbol de usuarios.
Eliminar	Suprime el usuario proxy seleccionado.

Utilización de campos de detalle de usuarios proxy

La siguiente tabla describe los campos que se encuentran en la vista **Detalle de usuario proxy** de Management Console:

Campo	Descripción
Usuario proxy	El nombre que se está especificando para un usuario que se está definiendo para el acceso proxy. Es el nombre de usuario con el que ese usuario iniciará la sesión con el servidor TELNET o FTP en el cortafuego IBM Firewall. Este usuario no tiene autorización de administración.
Dominio proxy	Especifica el nombre del dominio proxy del cortafuego.
Contraseña	Especifica la contraseña que debe utilizarse para iniciar la sesión con el dominio proxy del cortafuego.
Descripción	Especifica el texto que describe el usuario proxy. La descripción es tan solo un campo de datos opcional y el registro no la utiliza.
Shell remoto	Especifica el shell de inicio de sesión remota que debe utilizarse para el usuario proxy. La lista de opciones incluye **/bin/restrict.sh**, **/bin/csh**, **/bin/ksh /bin/bsh**, **/bin/oneact.sh** y una cadena de caracteres vacía.
Shell local	Especifica el shell de inicio de sesión local que debe utilizarse para el usuario proxy. La lista de opciones incluye **/bin/restrict.sh**, **/bin/csh**, **/bin/ksh /bin/bsh**, **/bin/oneact.sh** y una cadena de caracteres vacía.
Grupo por omisión	Especifica el grupo por omisión al que pertenece el usuario proxy. El administrador puede seleccionar el grupo de una lista de grupos presentados a los cuales pertenece el usuario proxy.

Autentificación de FTP seguro	Especifica el nivel de autentificación que necesita el usuario para utilizar FTP para acceder al cortafuego desde la red segura. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Autentificación de FTP remoto	Especifica el nivel de autentificación que necesita el usuario para utilizar FTP para acceder al cortafuego desde la red no asegurada. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Autentificación de Telnet segura	Indica si la identidad del usuario (cuando efectúa el inicio de sesión desde la red segura) debe autentificarse por algún medio. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Autentificación de Telnet remota	Indica si la identidad del usuario (cuando efectúa el inicio de sesión desde la red no asegurada) debe autentificarse por algún medio. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Autentificación de SOCK seguro	Especifica el método de autentificación de Socks, Versión 5, para conexiones de clientes Socks que procedan del área segura del cortafuego. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Autentificación de SOCK remoto	Especifica el método de autentificación de Socks, Versión 5, para conexiones de clientes Socks que procedan del área insegura del cortafuego. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.

Autentificación de HTTP seguro	Especifica un tipo de autentificación de par de ID de usuario y contraseña en peticiones de HTTP proxy de salida. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Autentificación local	Especifica el método de autentificación local. La lista de opciones incluye: **Contraseña de cortafuego**, **Permitir todos**, **Denegar todos**, **Tarjeta SecurID**, **Contraseña de conexión a NT**, **Suministrado por el usuario 1**, **Suministrado por el usuario 2**, **Suministrado por el usuario 3**, **Contraseña de conexión a AIX** y una cadena de caracteres vacía.
Tiempo desocupado antes de desconexión	Especifica el tiempo desocupado que se permite antes de desconectar al usuario.
Tiempo de aviso antes de desconexión	Especifica el tiempo de aviso que se permite antes de desconectar al usuario.
Contraseña válida	Especifica si debe pedirse al usuario, con un mensaje de solicitud, que entre una contraseña válida. IBM Firewall solicitará una contraseña al usuario.
Contraseña bloqueada	Especifica si la contraseña está bloqueada. El administrador debe dar a este campo el valor sí para impedir que un usuario utilice la autentificación de contraseña.

Adición de un usuario proxy

Para crear un usuario proxy:

1. Pulse el botón en el separador de tarea **Usuario proxy**.
2. Amplíe la región adecuada del árbol **Usuarios** y seleccione el usuario de Policy Director que desea convertir en un usuario proxy.
3. Rellene todos los campos de la vista **Detalle de usuario proxy**.
4. Pulse el botón **Guardar**.

Modificación de la información de un usuario proxy

Para modificar la información de un usuario proxy:

1. Pulse el botón en el separador de tarea **Usuario proxy**.
2. Amplíe la región adecuada de la vista de árbol **Usuarios** y seleccione un usuario proxy existente de la lista.

   El área Detalle de usuario proxy se rellenará con los datos actuales.
3. Entre los nuevos datos.
4. Pulse el botón **Guardar**.

Eliminación de un usuario proxy

Para eliminar un usuario proxy:

1. Pulse el botón en el separador de tarea **Usuario proxy**.
2. Amplíe la región adecuada de la vista de árbol **Usuarios** y seleccione un usuario proxy existente.

3. Pulse el botón del ratón en el botón **Eliminar**.

Utilización de los mandatos ivadmin policy para la gestión de usuarios proxy

Determinados mandatos **ivadmin policy** sólo se utilizan con usuarios proxy de Policy Director. Los mandatos **ivadmin policy** son un conjunto de mandatos de gestión que controlan la información general sobre políticas para usuarios de Policy Director y usuarios proxy. El administrador puede gestionar los siguientes atributos de políticas:

- "Gestión de políticas de inicio de sesión".
- "Gestión de políticas de contraseña" en la página 122

Una política (*policy*) define el conjunto de limitaciones impuestas a cuentas y contraseñas para mejorar la seguridad global del sistema. Estas limitaciones pueden imponerse generalmente (globalmente a todos los usuarios del sistema) o específicamente (sólo a un usuario especificado). Si se ha aplicado una política específica a un usuario, dicha política específica tendrá prioridad sobre cualquier otra política general que también pueda haberse definido. La prioridad se aplica independientemente de si la política especificada es más o menos restrictiva que la política general.

Gestión de políticas de inicio de sesión

Los siguientes mandatos **ivadmin policy** permiten al administrador de IBM SecureWay Boundary Server gestionar políticas relacionadas con el inicio de sesión.

Utilice los mandatos **policy** de tareas de gestión relacionadas con el inicio de sesión para crear nuevas políticas de inicio de gestión. Estas políticas se aplicarán a todos los usuarios.

Para políticas relacionadas con el inicio de sesión, Policy Director define el tiempo relativo como DDD-hh:mm:ss, y define el tiempo absoluto como AAAA-MM-DD-hh:mm:ss cuando se refiere a mandatos **policy** de tareas de gestión.

Mandato	Descripción
policy {set | get} disable-time-interval [*número*]	

	Especifica la cantidad de tiempo (en segundos) que debe estar inhabilitada una cuenta después de haber alcanzado el número máximo de intentos de inicio de sesión fallidos.
	
	El argumento *número* es el número de segundos que debe inhabilitarse la cuenta.
	
	Ejemplos:
	`ivadmin> policy set disable-time-interval 3`
	
	O:
	`ivadmin>`
	`policy get disable-time-interval`

policy {set | get} max-login-failures [*número*]	

	Crea una nueva política o visualiza un política existente que indica el número máximo de intentos incorrectos de inicio de sesión permitidos. El argumento *número* es el número máximo de intentos incorrectos de inicio de sesión que se permitirá.
	
	Ejemplos:
	`ivadmin> policy set max-login-failures 5`
	
	O:
	`ivadmin> policy get max-login-failures`

Gestión de políticas de contraseña

Los siguientes mandatos **ivadmin policy** permiten al administrador de IBM SecureWay Boundary Server gestionar políticas relacionadas con las contraseñas.

Para políticas relacionadas con las contraseñas, Policy Director define el tiempo relativo como DDD-hh:mm:ss cuando se refiere a mandatos **policy** de tareas de gestión.

Mandato	Descripción
policy {set | get} max-password-age [*tiempo-relativo*]	

	Gestiona la política que controla el tiempo máximo que debe transcurrir para que una contraseña deba cambiarse. El argumento *tiempo-relativo* es el tiempo especificado—expresado en días, horas y minutos, con el siguiente formato: `DDD-hh:mm:ss`
	
	Ejemplos:
	`ivadmin> policy set max-password-age 031-08:30:00`
	
	O:
	`ivadmin> policy get max-password-age`

policy {set | get} max-password-repeated-chars [*número*]	

	Especifica el número máximo de caracteres que puede repetirse secuencialmente en una contraseña de usuario.
	
	Ejemplos:
	`ivadmin> policy set max-password-repeated-chars 3`
	
	Utilizando este ejemplo de tres caracteres repetidos como máximo, `deptfff` puede definirse como contraseña porque no sobrepasa tres caracteres “f” repetidos. La contraseña `deptffff` no podría establecerse como contraseña porque cuatro caracteres “f” sobrepasan el límite de tres caracteres repetidos.
	
	O:
	`ivadmin> policy get max-password-repeated-chars`

policy {set | get} min-password-alphas [*número*]	

	Especifica el número mínimo de caracteres alfanuméricos que debe utilizarse en una contraseña de usuario.
	
	Ejemplos:
	`ivadmin> policy set min-password-alphas 5`
	
	Utilizando este ejemplo, una contraseña debe contener como mínimo cinco caracteres alfanuméricos.
	
	O:
	`ivadmin> policy get min-password-alphas`

policy {set | get} min-password-non-alphas [*número*]	

	Especifica el número mínimo de caracteres no alfanuméricos que debe utilizarse en una contraseña de usuario.
	
	Ejemplos:
	`ivadmin> policy set min-password-non-alphas 1`
	
	Utilizando este ejemplo, una contraseña debería contener como mínimo un carácter alfanumérico para ser válida.
	
	O:
	`ivadmin> policy get min-password-non-alphas`

policy {set | get} min-password-different-chars [*número*]	

	Especifica el número mínimo de caracteres distintos que debe utilizarse en una contraseña de usuario.
	
	Ejemplos:
	`ivadmin> policy set min-password-different-chars 3`
	
	Utilizando este ejemplo, una contraseña debería contener como mínimo tres caracteres distintos para ser válida. Si la contraseña especificada es ddddyyyy, no sería válida porque sólo contiene dos caracteres distintos (d e y).
	
	O:
	`ivadmin> policy get min-password-different-chars`

policy {set | get} min-password-length [*número*]	

	Especifica la longitud mínima, en caracteres, de una contraseña. El argumento *número* indica la longitud mínima autorizada para una contraseña.
	
	Ejemplos:
	`ivadmin> policy set min-password-length 8`
	
	O:
	`ivadmin> policy get min-password-length`

policy {set | get} min-password-reuse-num [*número*]	

	Especifica el número de veces que debe cambiarse una contraseña para poder utilizar de nuevo una contraseña utilizada anteriormente.
	
	Ejemplos:
	`ivadmin> policy set min-password-reuse-num 3`
	
	O:
	`ivadmin> policy get min-password-reuse-num`

policy {set | get} min-password-reuse-time [*tiempo-relativo*]	

	Especifica el tiempo mínimo que debe pasar para poder reutilizar una contraseña.
	
	El argumento *tiempo-relativo* indica el tiempo mínimo, expresado en días, horas y minutos con este formato (`DDD-hh:mm:ss`). Un usuario no puede utilizar de nuevo la misma contraseña dentro de un límite de tiempo especificado (por ejemplo 60 días o `060-00:00:00`).
	
	Ejemplos:
	`ivadmin> policy set min-password-reuse-time 060-00:00:00`
	
	O:
	`ivadmin> policy get min-password-reuse-time`

policy {set | get} password-expiry-date [*tiempo-relativo*]	

	Especifica la fecha y la hora en que la contraseña debe caducar.
	
	Ejemplos:
	`ivadmin> policy set password-expiry-date 031-08:30:00`
	
	O:
	`ivadmin> policy get password-expiry-date`

policy {set | get} password-expiry-warn [*número*]	

	Avisa al usuario de que la contraseña está a punto de caducar. El argumento *número* indica cuántos días antes de la fecha de caducidad empiezan los avisos (por ejemplo, cuatro días antes de que la contraseña vaya a caducar).
	
	Ejemplos:
	`ivadmin> policy set password-expiry-warn 4`
	
	O:
	`ivadmin> policy get password-expiry-warn`

Capítulo 10. Gestión de servidores de Policy Director

Este capítulo trata de las tareas generales para administrar y configurar el conjunto de servidores de Policy Director. También se explican los archivos de configuración que se aplican a cada servidor.

Este capítulo incluye los siguientes temas:

Presentación de los servidores de Policy Director

Policy Director Server consta de los siguientes procesos (daemons) de servidor:

- Security Server (secd)
- Security Manager (secmgrd)
- Authorization Server (ivacld)
- Management Server (ivmgrd)
- Directory Service Broker (DSB)

Estos servidores se configuran automáticamente durante la instalación del producto.

El **Security Server (secd)** de Policy Director es únicamente un DCE Server. El Security Server proporciona servicios de autentificación. El Security Server también mantiene una base de datos de registros centralizada. El registro de usuarios puede ser LDAP o DCE. Si el registro de usuarios es DCE, la base de datos de registros centralizada contiene información de contabilidad de todos los usuarios válidos que participan del dominio seguro.

EL **Security Manager (secmgrd)** contiene los Security Server WebSEAL y NetSEAL.

El **Authorization Server (ivacld)** atiende las peticiones de autorización de cualquier aplicación de terceros que utilice la API de autorizaciones de Policy Director en modalidad remota. Normalmente, Authorization Server requiere muy pocas operaciones de administración o configuración.

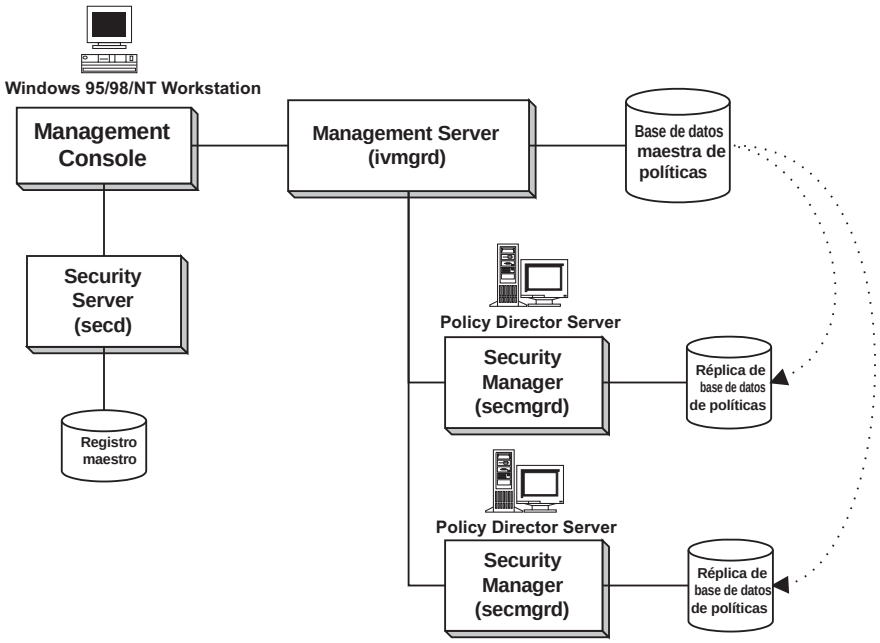
Management Server (ivmgrd) gestiona la base de datos primaria de ACL y mantiene información sobre ubicaciones de los otros servidores WebSEAL y NetSEAL de un dominio seguro. Normalmente, Management Server requiere muy pocas operaciones de administración o configuración.

Directory Services Broker (DSB) se distribuye como parte del paquete de Management Server (IVMgr). Management Console requiere un Directory Services Broker en el dominio seguro cuando se ejecuta en estaciones de trabajo con Windows NT, Windows 95 o Windows 98. Normalmente, Directory Services Broker no requiere operaciones de administración ni de configuración tras la instalación inicial.

Puntos a tener en cuenta con los servidores

Los puntos a tener en cuenta con los servidores de Policy Director son, entre otros:

- Debe haber una sola instancia de Management Server y de sus bases de datos de autorizaciones (ACL) primaria en cualquier dominio seguro.
- Management Server reproduce su base de datos de ACL para todos los otros servidores de Policy Director del dominio seguro.
- En todos los servidores de Policy Director reside un Security Manager, con detecciones WebSEAL y NetSEAL.
- Cada Security Manager aplica una política de control de accesos basada en la información de la réplica de la base de datos de autorizaciones o de ACL.



Visión general de las herramientas de administración de servidores

La administración del servidor puede ejecutarse a través de las siguientes interfaces:

- Programa de utilidad **ivadmin**
- Programa de utilidad **wandmgr** (sólo WebSEAL)
- Scripts de UNIX
- Panel de control Servicios de Windows NT

Este capítulo explica como utilizar cada una de estas interfaces.

ivadmin, **wandmgr** y los scripts de arranque proporcionan interfaces de línea de mandatos. Resultan útiles cuando se automatizan las tareas de administración del servidor dentro de los scripts de shell.

Management Console, ivadmin y wandmgr pueden utilizarse remota o localmente. Los scripts de arranque deben administrarse localmente.

Cuando se encuentran y corrigen problemas, los programas de utilidad de línea de mandatos pueden proporcionar información sobre el estado y controlar servidores individuales.

Programa de utilidad ivadmin

Policy Director facilita el programa de utilidad de línea de mandatos **ivadmin** para llevar a cabo tareas de servidor más avanzadas. Utilice **ivadmin**:

- Para llevar a cabo todas las tareas de Management Console indicadas en la sección anterior
- Para visualizar el estado de servidores

Programa de utilidad wandmgr

El programa de utilidad de línea de mandatos **wandmgr** es una herramienta de Policy Director WebSEAL que se utiliza para efectuar tareas avanzadas de autorización de clientes de la Web y de gestión de la antememoria como, por ejemplo:

- Visualizar el estado de la antememoria de objetos de la Web.
- Suprimir antememorias de objetos de la Web de la memoria.

Scripts de UNIX

Policy Director utiliza scripts para detener e iniciar automáticamente servidores durante un arranque del sistema y para visualizar el estado de servidores. Estos scripts pueden iniciarse manualmente:

- Para detener servidores.
- Para visualizar el estado de servidores.
- Para iniciar servidores.

Panel de control Servicios de Windows NT

Utilice el Panel de control Servicios de Windows NT:

- Para iniciar un servidor.
- Para detener un servidor.
- Para introducir una pausa en el servidor (suspenderlo).
- Para que un servidor en pausa continúe (se reanude).
- Para listar servidores configurados.

Archivos de configuración del servidor

Los servidores de Policy Director utilizan archivos de configuración para indicar la funcionalidad:

Nombre de servidor	Proceso	Archivo de configuración

Security Manager	**secmgrd**	**UNIX:**
		`/opt/intraverse/secmgr/lib/secmgrd.conf`
		
		Windows:
		`\Archivos de programa\ibm\Policy Director\secmgr\lib\secmgrd.conf`

Management Server	**ivmgrd**	**UNIX:**
		`/opt/intraverse/ivmgrd/lib/ivmgrd.conf`
		
		Windows:
		`\Archivos de programa\ibm\Policy Director\ivmgrd\lib\ivmgrd.conf`

Authorization Server	**ivacld**	**UNIX:** /opt/intraverse/ivacld/lib/ivacld.conf **Windows:** \Archivos de programa\ibm\Policy Director\ivacld\lib\ivacld.conf

Los archivos de configuración cumplen con las normas de American National Standard Code for Information Interchange (ASCII) y pueden editarse utilizando un editor normal. Las entradas de los archivos tienen el siguiente formato:

```
parámetro=valor
```

Durante la instalación inicial de un Policy Director Server se definen valores por omisión para la mayoría de parámetros. Algunos parámetros son estáticos y no cambian nunca; otros pueden ajustarse o añadirse para configurar la funcionalidad del servidor y optimizar su rendimiento.

Nota: Después de haber editado un archivo de configuración, deberá reiniciar Policy Director Server para que los cambios surtan efecto.

Cada archivo contiene **secciones** con valores para una categoría determinada de configuración. Las etiquetas de las secciones están entre corchetes [ ].

Por ejemplo, la sección `[intraverse]` de iv.conf define los valores generales de la configuración de Policy Director que se aplican a todo el dominio seguro. La sección `[wand-mime-types]` define las definiciones de tipos de MIME soportadas por Policy Director WebSEAL en el sistema local.

Los archivos están comentados para explicar la utilización de cada parámetro. Cuando deba cambiar algún valor de la configuración, edite cuidadosamente los archivos para asegurarse de preservar su integridad.

UNIX: Detención e inicio de Policy Director Servers

Normalmente, el inicio y la detención de los procesos del servidor se lleva a cabo mediante scripts automatizados que se ejecutan durante el arranque y el cierre del sistema.

El administrador también puede utilizar scripts para iniciar y detener manualmente los procesos del servidor. Esta técnica resulta útil para personalizar una instalación o para buscar y corregir problemas. Los scripts sólo pueden aplicarse en la máquina local. Utilice Management Console o el programa de utilidad **ivadmin** para detener e iniciar servidores de forma remota.

Los servidores de Policy Director pueden iniciarse y detenerse todos a la vez o de uno en uno. Normalmente, los servidores deben iniciarse y detenerse en el orden correcto.

El proceso de peticiones Cell Directory Services (CDS) en nombre de clientes NetSEAT requiere Directory Services Broker. (La versión Windows de Management Console utiliza el cliente NetSEAT.)

Detención utilizando el script iv

Utilice el script iv para detener todos los servidores Policy Director de una máquina determinada en el orden correcto:

AIX:

```
# /etc/iv/iv stop
```

Solaris:

```
# /etc/init.d/iv stop
```

Este script tan solo efectúa la detención en el siguiente orden: ivacld, secmgrd e ivmgrd. El script espera a que todos los servidores se hayan detenido para devolver un mensaje.

Cierre manual

Los servidores también pueden detenerse inmediatamente utilizando el mandato **kill**:

`# kill <pid>`	Fuerza al servidor a concluir limpiamente.
`# kill -9 <pid>`	Cierra abruptamente el servidor, sin ninguna limpieza.

Cierre los Policy Director Servers en el siguiente orden:

1. Directory Services Broker (DSB)
2. Authorization Server (ivacld)
3. Security Manager (secmgrd)
4. Management Server (ivmgrd)

Inicio utilizando el script iv

Utilice el script iv para iniciar todos los servidores Policy Director de una máquina determinada en el orden correcto:

AIX:

```
# /etc/iv/iv start
```

Solaris:

```
# /etc/init.d/iv start
```

Este script tan solo efectúa el inicio en el siguiente orden: ivmgrd, secmgrd e ivacld. El script espera a que todos los servidores se hayan iniciado para devolver un mensaje.

Inicio manual

Los servidores pueden iniciarse manualmente, de uno en uno, iniciándolos directamente. El servidor se inicializa solo. Si la operación es correcta, el servidor se coloca a sí mismo como daemon.

Debe ejecutar los mandatos de arranque como usuario de administración como, por ejemplo, root o ivmgr. Inicie los Policy Director Servers en el siguiente orden:

1. Management Server (ivmgrd):
   ```
   # /opt/intraverse/ivmgrd/bin/ivmgrd
   ```
2. Security Manager (secmgrd):
   ```
   # /opt/intraverse/secmgr/bin/secmgrd
   ```
3. Authorization Server (ivacld):
   ```
   # /opt/intraverse/ivacld/bin/ivacld
   ```
4. Directory Services Broker (DSB):
   ```
   # /opt/intraverse/broker/bin/dsb
   ```

Visualización del estado del servidor

Para saber si un servidor está funcionando, utilice el siguiente mandato:

AIX:

```
# /etc/iv/iv status
```

Solaris:

```
# /etc/init.d/iv status
```

```
DCE Servers:
Servidor                  Habilitado              Funcionando
dced                      sí                      sí
secd                      -                       sí
cdsd                      -                       sí
dtsd                      -                       sí
dsb                       -                       sí

Policy Director Servers:
Servidor                  Habilitado              Funcionando
ivmgrd                    sí                      sí
secmgrd                   sí                      sí
ivacld                    sí                      sí
```

Windows: detención e inicio de Policy Director Servers

Utilice el panel de control Servicios de Microsoft Windows NT para iniciar y detener manualmente los procesos de los servidores. Esta técnica puede resultar útil para personalizar una instalación o para buscar y corregir problemas. Para utilizar este programa de utilidad es necesario tener privilegios administrativos.

Los servidores de Policy Director pueden iniciarse y detenerse todos a la vez o de uno en uno. Normalmente, los servidores deben detenerse e iniciarse en el orden correcto.

Policy Director AutoStart Service inicia automáticamente cada Policy Director Server siempre que se reinicia (rearranca) el sistema. Cuando los servidores se inician, AutoStart Service se cierra.

Para iniciar y detener manualmente Policy Director Servers individuales utilice el Panel de control Servicios de Windows NT:

1. Abra el Panel de control de Windows.
2. Efectúe una doble pulsación en el icono **Servicios**.

   Aparecerá el recuadro de diálogo Servicios. Pueden aparecer, entre otros, los siguientes servicios:

   ```
   Servicio                                Estado          Arranque
   Director Services Broker                Iniciado        Automático
   Policy Director Authorization Server    Iniciado        Manual
   Policy Director Auto-Start Service      Iniciado        Automático
   Policy Director Management Server       Iniciado        Manual
   Policy Director Security Manager        Iniciado        Manual
   Policy Director X.509 Authorization Server  Iniciado    Manual
   ```
3. En el cuadro de lista, seleccione los servidores de Policy Directory con la secuencia indicada en los pasos 4 y 5 en la página 131.
4. Detenga los servidores en el siguiente orden:
   - Security Manager

- Management Server
- Directory Services Broker

5. Inicie los servidores en el siguiente orden:
   - Directory Services Broker
   - Management Server
   - Security Manager
   - Authorization Server
6. Pulse el botón del ratón en el botón de opción de control adecuado (**Iniciar, Detener, Arrancar**) de la derecha del recuadro.
7. Para impedir que Policy Director AutoStart Service arranque automáticamente un Policy Director Server, utilice el botón de opción **Arranque**. Este botón inhabilita el Policy Director Server.

Automatización del inicio del servidor durante el arranque

La sección [intraverse] del archivo de configuración iv.conf contiene parámetros para automatizar o no el arranque del servidor.

Durante la instalación, se puede configurar el daemon de Security Server (secmgrd) para que se inicie automáticamente tras cada reinicio del sistema.

```
[intraverse]
boot-start-secmgrd = yes
```

Para impedir el arranque automático de secmgrd, indique:

```
boot-start-secmgrd = no
```

Cuando se instala el paquete IVMgr, el daemon de Policy Director Management Server (ivmgrd) se inicia automáticamente después de cada reinicio del sistema.

```
[intraverse] boot-start-ivmgrd = yes
```

Para impedir el arranque automático de ivmgrd, indique:

```
boot-start-ivmgrd = no
```

Nota: Cada dominio seguro (célula) requiere un daemon de Policy Director Management Server. No instale ni ejecute **ivmgrd** en más de un servidor por célula.

Cuando se instala el paquete IVAcld, el daemon de Policy Director Authorization Server se inicia automáticamente tras cada reinicio del sistema.

```
[intraverse]
boot-start-ivacld = yes
```

Para impedir el arranque automático de **ivacld**, indique:

```
boot-start-ivacld = no
```

Configuración de hebras de trabajo de RPC

El número de hebras de trabajo configuradas especifica el número de peticiones simultáneas entrantes que un servidor puede atender. Cuando todas las hebras de trabajo están ocupadas, Policy Director coloca en el almacenamiento intermedio las otras conexiones que llegan hasta que una hebra de trabajo queda disponible.

Puede definir el número de hebras de forma que sea suficiente para atender a las peticiones de conexión entrantes. Configure cuidadosamente el número de hebras de trabajo ya que éste puede incidir en el rendimiento.

Los parámetros de configuración no imponen un límite superior en el número de conexiones simultáneas. Estos parámetros especifican simplemente el número de hebras disponibles para atender a una cola de trabajos potencialmente ilimitada.

La selección del número óptimo de hebras de trabajo depende de que se asimile la cantidad y el tipo de tráfico de la red.

Al aumentar el número de hebras, disminuye el tiempo medio que se tarda en finalizar las peticiones. Sin embargo, al aumentar el número de hebras se incrementa la actividad general del servidor y el tiempo medio que se tarda en atender una petición aumenta de nuevo.

Cada archivo de configuración de los servidores secmgrd, ivmgrd e ivacld contiene los siguientes parámetros para configurar las hebras de trabajo de RPC:

- El número máximo de hebras de trabajo de RPC
- La puerta TCP para estar a la escucha de RPC entrantes
- La puerta del protocolo de datagramas de usuario (UDP) para estar a la escucha de RPC entrantes

Nombre de servidor	Proceso	Archivo de configuración
Security Manager	**secmgrd**	secmgrd.conf
Management Server	**ivmgrd**	ivmgrd.conf
Authorization Server	**ivacld**	ivacld.conf

Definición de la agrupación de hebras de trabajo de RPC

Los Policy Director Servers utilizan hebras de trabajo de RPC para procesar:

- Peticiones de RPC entrantes procedentes de clientes NetSEAT
- Actualizaciones de la base de datos generadas por tareas administrativas realizadas desde Management Console

El parámetro de máximas hebras de trabajo de RPC, que se encuentra en cada archivo de configuración de servidor, contiene el siguiente valor por omisión:

```
max-rpc-worker-threads = 10
```

Considere la posibilidad de aumentar este valor cuando Policy Director Server maneje un gran número de clientes NetSEAT.

Configuración de servidores para peticiones entrantes de RPC

La siguiente tabla lista los valores de puertas por omisión para la escucha de RPC en cada servidor:

Servidor	Archivo de configuración	Parámetros de puertas con valores por omisión
secmgrd	secmgrd.conf	`rpc-tcp-port = 6052 rpc-udp-port = 0`
ivmgrd	ivmgrd.conf	`tcp-rpc-port = 6032 udp-rpc-port = 0`
ivacld	ivacld.conf	`tcp-rpc-port = 6031 udp-rpc-port = 0`

Un valor de puerta cero (0) inhabilita la escucha de RPC en esa puerta. Es muy aconsejable que utilice TCP para estar a la escucha. Active las puertas UDP únicamente cuando sea absolutamente necesario.

Puede definir distintas puertas según sus necesidades.

Ejemplo para secmgrd:

```
rpc-udp-port = 6052
```

TCP y UDP escuchan ahora en la misma puerta.

Capítulo 11. Gestión del servicio de autorizaciones

Policy Director Authorization Service pone en vigor la política de seguridad de una red controlando el proceso de toma de decisiones de autorización. Puede ampliar las posibilidades de autorización de Policy Director de varias formas: definiendo e incorporando espacios de nombres adicionales, definiendo nuevos permisos de control de accesos y acomodando *servicios de autorizaciones externos* de terceros. Este capítulo trata de las tareas comunes necesarias para configurar, mantener y ampliar Policy Director Authorization Service.

Este capítulo incluye los siguientes temas:

Definición de espacios de nombres de aplicaciones de terceros

Los siguientes factores definen una política de seguridad de Policy Director:

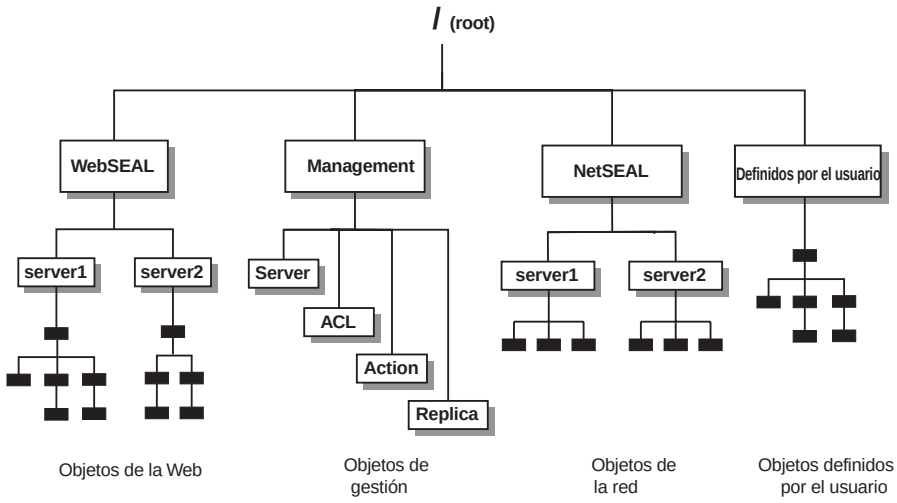
- ¿Quién podrá participar del dominio seguro?
- ¿Qué objetos deben protegerse?
- ¿Qué normas deben proteger dichos objetos?

El espacio de nombres de objetos protegidos es la representación lógica y jerárquica de los recursos que pertenecen al dominio seguro. Los objetos del espacio de nombres representan los recursos del sistema que deben protegerse (como archivos y puertas). Para proteger cualquier recurso del dominio seguro se unen plantillas de políticas (ACL) a las representaciones de objetos de dichos recursos.

El espacio de nombres de objetos protegidos utiliza dos tipos de objetos:

Objetos contenedores
: Los objetos contenedores son designaciones estructurales que permiten organizar el espacio de nombres jerárquicamente en distintas regiones funcionales. Los objetos contenedores contienen objetos de recursos.

Objetos de recursos
: Los objetos de recursos son las representaciones de recursos reales del sistema (como servicios, archivos y programas) en el dominio seguro.



Policy Director permite ampliar sus servicios de autorizaciones a objetos que pertenecen a un espacio de nombres de terceros. La integración de un espacio de nombres de terceros con Policy Director requiere estas operaciones:

- Describir a Policy Director el espacio de nombres de la aplicación de terceros.
- Aplicar plantillas de políticas (ACL) a cualquier objeto del espacio de nombres que requiera protección.

El contenido de un espacio de nombres de terceros se describe a Policy Director a través de un archivo de correlación especial. Ese archivo indica los objetos de recursos específicos que pertenecen al espacio de nombres de terceros e indica su relación jerárquica.

Además, debe definirse el objeto contenedor root que contiene el espacio de nombres de terceros. El nombre del objeto contenedor root aparecerá como parte del espacio de nombres de Policy Director cuando Management Console lo visualice (separador Espacio de objetos). Los objetos contenedores estándar existentes estándar en Policy Director son, entre otros, /WebSEAL, /NetSEAL y /Management.

El archivo de configuración de Management Server (ivmgrd.conf) define el nombre del objeto contenedor de terceros y la ubicación del archivo de correlación.

Nombre del objeto contenedor root y ubicación del archivo de correlación

La sección [object-spaces] del archivo de configuración de Management Server (ivmgrd.conf) define estos dos elementos:

- El nombre del objeto contenedor root del espacio de nombres de terceros.
- La ubicación del archivo de correlación.

Cada entrada tiene el siguiente formato:

root del espacio de objetos = archivo de correlación

Donde:

root del espacio de objetos El nombre del objeto contenedor que contiene el espacio de nombres de terceros.

archivo de correlación El nombre de la vía de acceso completa al archivo de correlación. El archivo de correlación puede encontrarse en cualquier lugar.

El siguiente ejemplo define un objeto contenedor de terceros (Notes) y la ubicación de un archivo de correlación: notemap.txt:

UNIX: /Notes = /opt/intraverse/lib/notemap.txt

Windows: /Notes = C:\Archivos de programa\IBM\Policy Director\lib\notemap.txt

Nota: Para incorporar las modificaciones que desee al archivo ivmgrd.conf deberá detener y reiniciar Management Server.

Formato del archivo de correlación

El archivo de correlación que describe el espacio de nombres de terceros es un archivo de texto ASCII. Cada línea del archivo es un nombre de vía de acceso absoluta que representa a cada objeto de recurso del espacio de nombres. El archivo de correlación sólo lista objetos de recursos; Policy Director implica objetos contenedores procedentes de los nombres de vías de acceso.

Las normas para archivos de correlación adicionales son, entre otras:

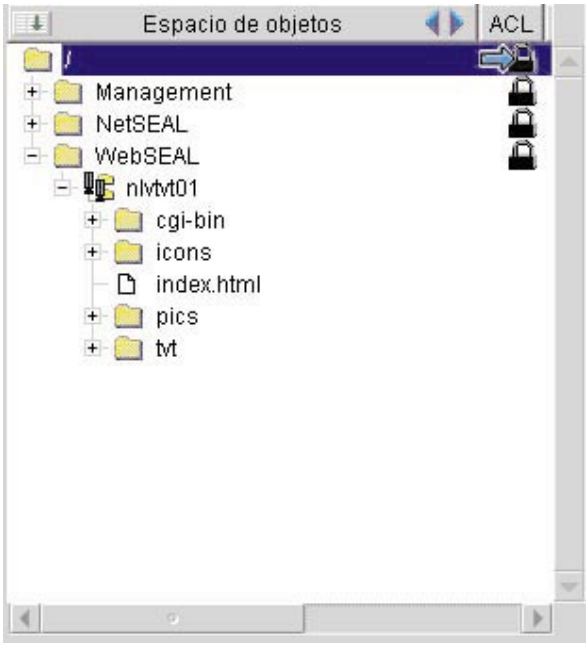
- Listar únicamente un nombre de objeto y vía de acceso por línea.
- Los nombres de vías de acceso empiezan siempre por una barra inclinada (/).

Ejemplo de archivo de correlación:

```
/Forum/public/mail
/Forum/public/reference
/Forum/public/chat
/Forum/documents/style
/Forum/documents/guide
/Forum/documents/manual
/Forum/private/mail
/Forum/private/notes
/Forum/private/bulletins
```

Visualización jerárquica en Management Console

La siguiente pantalla de Management Console es el resultado del ejemplo de archivo de correlación descrito en el apartado “Formato del archivo de correlación”.



Definición de permisos ACL personalizados

Policy Director se basa en plantillas de políticas para especificar las condiciones necesarias para realizar una operación sobre un objeto protegido. Policy Director utiliza un tipo específico de plantilla de política llamado lista de control de accesos (Access Control List, ACL).

Entradas de ACL

Se puede unir una ACL a un objeto. Una vez conectadas, las entradas de la ACL indican qué operaciones permite realizar Policy Director sobre dicho objeto y quién puede llevar a cabo las operaciones. Una entrada de ACL incluye, entre otros:

- El tipo de usuario o el tipo de grupo

  Existe también un tipo para usuarios no autentificados y autentificados por cualquiera.
- Identidad de usuario o identidad de grupo exclusivas.
- Permisos

Permisos

Policy Director utiliza un conjunto estándar de permisos que cubren una amplia gama de operaciones. Los permisos se representan mediante caracteres ASCII individuales imprimibles. En Management Console (separador **ACL**), Policy Director visualiza cada permiso con una etiqueta que describe la operación que dirige. Además, Policy Director agrupa las ACL, según su uso, en un espacio de nombres determinado o para que puedan utilizarse en todo el espacio de nombres. Entre estas categorías de grupos están las siguientes: Base, Genérico (Generic), WebSEAL, NetSEAL.

Operaciones sobre un objeto

El software de aplicaciones contiene normalmente una o más operaciones que se realizan sobre objetos protegidos. Para que la operación solicitada pueda llevarse a cabo, las aplicaciones efectúan primero llamadas al servicio de autorizaciones. La

llamada se realiza con la API de autorizaciones de Policy Director tanto para aplicaciones de Policy Director como de terceros.

La información se encuentra en la ACL que protege al objeto. El servicio de autorizaciones utiliza la información para efectuar una simple respuesta sí o no a la pregunta ¿Tiene este usuario (grupo) el permiso "r" (por ejemplo) sobre el objeto solicitado?

Es importante tener en cuenta que el servicio de autorizaciones no sabe nada sobre la operación que requiere el permiso de lectura (r). Lo único que le preocupa es la presencia (o ausencia) del permiso de lectura (r). El permiso de lectura (r) se encuentra en la entrada de ACL del usuario o grupo que efectúa la petición.

Este permiso es una característica muy potente de Policy Director Authorization Service. El servicio es completamente independiente de las operaciones que van a solicitarse y, por este motivo, es fácil extender las ventajas del servicio de autorizaciones a las aplicaciones de terceros.

Requisitos para permisos personalizados

Todo el repertorio de permisos estándar de Policy Director está disponible para aplicaciones de terceros. Una aplicación de terceros puede utilizar los permisos de Policy Director. Si lo hace, la operación asociada deberá ser igual que la operación real realizada normalmente por Policy Director. Por ejemplo, una operación que requiera un acceso de sólo lectura a un objeto protegido deberá utilizar el permiso de lectura (r).

Nota: Una aplicación de terceros puede utilizar un permiso estándar de Policy Director para una operación no relacionada con la utilización normal ya que Policy Director no conoce ni se preocupa de la operación. Sin embargo, esto causaría dificultades a un administrador que debería distinguir entre dos usos distintos de un mismo permiso.

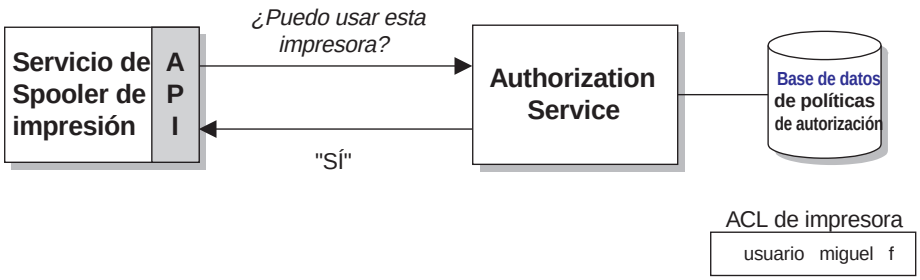
Una aplicación de terceros podría utilizar una operación que no estuviese representada en el conjunto de permisos estándar. Si es así, Policy Director le permite definir un nuevo permiso. La aplicación utilizaría entonces ese servicio que el servicio de autorizaciones reconocería.

Ejemplo:

El requisito que implica este ejemplo es proteger un determinado dispositivo de impresora contra utilizaciones no autorizadas. Con la API de autorizaciones de Policy Director se escribirá un servicio de spooling de impresión de terceros. Ese servicio de spooling de impresión llamará al servicio de autorizaciones para que efectúe comprobaciones de ACL cuando se reciban peticiones para la impresora.

Los permisos estándar de Policy Director no incluyen ningún permiso para la protección de impresoras. El permiso de impresión que acaba de crearse en este ejemplo debería proteger la impresora.

A partir de ese momento habrá una ACL unida al objeto de impresora. Si un usuario solicita la utilización de la impresora protegida, deberá tener una entrada de ACL que contenga el permiso de impresión. El servicio de autorizaciones devolverá una respuesta favorable si existe el permiso de impresión y la operación de impresión prosigue. Si el servicio de autorizaciones no encuentra un permiso de impresión, la operación de impresión no tendrá autorización para proseguir.



Gestión de permisos

Como administrador de Policy Director, podrá gestionar permisos como se indica a continuación:

- Añadiendo permisos personalizados
- Suprimiendo permisos personalizados
- Visualizando todos los permisos disponibles

Creación de un permiso personalizado

Los mandatos **ivadmin action** se utilizan para crear, eliminar y listar permisos. Es necesario estar conectado como administrador de Policy Director para poder utilizar el programa de utilidad **ivadmin**.

Utilice la siguiente sintaxis de mandato para crear un nuevo permiso personalizado:

```
ivadmin> action create nombre descripción tipo-de-acción
```

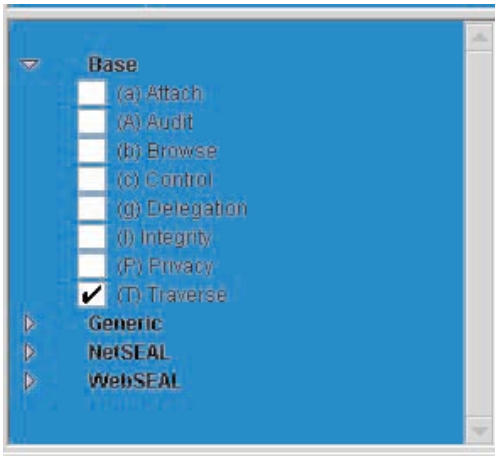
Donde:

`nombre`	El carácter ASCII imprimible que representa al permiso.
`descripción`	La etiqueta descriptiva que aparece a la derecha del carácter en la pantalla de Management Console (separador ACL).
`tipo-de-acción`	La categoría de organización donde aparece este permiso en la pantalla de Management Console (separador ACL).

Por ejemplo, si se escribe:

```
ivadmin> action create f print Devices
```

esta nueva entrada aparecerá en el panel de gestión de ACL de Management Console.



Eliminación de un permiso personalizado

Utilice la siguiente sintaxis de mandato para eliminar un permiso personalizado:

```
ivadmin> action delete nombre
```

Por ejemplo:

```
ivadmin> action delete f
```

Listado de todos los permisos disponibles

Utilice la siguiente sintaxis de mandato para lista todos los permisos disponibles:

```
ivadmin> action list
```

Verá una lista de permisos parecida a ésta:

```
p "Proxy" NetSEAL
r "Read" WebSEAL
v "View" Generic
x "Execute" WebSEAL
A "Audit" Base
a "Attach" Base
b "Browse" Base
c "Control" Base
C "Connect" NetSEAL
d "Delete" Generic
f "Print" Devices
g "Delegation" Base
I "Integrity" Base
l "List Directory" WebSEAL
m "Modify" Generic
P "Privacy" Base
s "Server Admin" Generic
T "Traverse" Base
...
```

Definición de servicios de autorizaciones externos

Un *servicio de autorizaciones externo* permite imponer controles de autorización adicionales y condiciones que suplementen el proceso de autorizaciones estándar de Policy Director. Un programa servidor de autorizaciones distinto dicta estos controles y condiciones adicionales.

Policy Director Authorization Service crea automáticamente la función de autorización externa. Si se configura un servicio de autorizaciones externo, Policy Director Authorization Service simplemente incorporará los nuevos controles y condiciones a su proceso de evaluación.

La puesta a punto de un servicio de autorizaciones externo requiere la realización de estas dos operaciones generales:

1. Escribir un programa servidor al que podrá hacerse referencia durante una toma de decisión de autorización.

   Consulte el manual *Policy Director Programmer's Guide and Reference*.
2. Registrar el servicio de autorizaciones externo con Policy Director.

   Consulte el apartado "Registro de un servicio de autorizaciones externo".

Después de registrar el servicio, en la consola de Policy Director Management Console aparecerá un nuevo permiso representándolo. A partir de ese momento, podrá utilizar ese permiso en cualquier entrada de la ACL.

Cuando Policy Director encuentre ese permiso durante una comprobación de autorización, consultará al servicio de autorizaciones externo para tomar decisiones adicionales de autorización.

Si desea ver más información sobre este tema, consulte el apartado "Posibilidad de autorización externa" en la página 52.

Registro de un servicio de autorizaciones externo

Utilice el mandato **ivadmin server register** para informar a Policy Director Authorization Service de la existencia y ubicación de un servicio de autorizaciones externo.

Se utiliza la siguiente sintaxis:

```
ivadmin> server register externauth nombre-servidor ubicación-en
principal-servidor
         car-acción nombre-acción
```

Donde:

nombre-servidor	Un nombre (o etiqueta) para este servicio de autorizaciones externo. Es el nombre que aparece en la pantalla del espacio de objetos de Management Console y en el mandato ivadmin server list.
ubicación-en	La entrada de RPC en el espacio de nombres CDS donde el servidor de autorizaciones externo exporta los enlaces de RPC.
principal-servidor	El nombre de LDAP o el nombre de principal DCE correspondiente al proceso del servidor de autorizaciones externo.
car-acción	El carácter que indica el permiso utilizado en una ACL para indicar la utilización del servicio de autorizaciones externo para decisiones suplementarias sobre autorizaciones.
nombre-acción	La etiqueta descriptiva que aparece a la derecha del carácter en la pantalla de Management Console (separador ACL).

Este mandato produce una categoría de organización de ACL por omisión que se denomina *autorización externa*. Management Console utiliza la categoría de organización de ACL por omisión cuando visualiza las ACL. Bajo esta categoría aparecen los permisos de todos los servicios de autorizaciones externos.

Por ejemplo, si se escribe:

```
ivadmin> server register externauth timechecker /.:/subsys/timechk
         t-checker k time-check
```

Se registra un servidor de autorizaciones externo llamado timechecker con el servicio de autorizaciones. La entrada de RPC en el espacio de nombres CDS donde timechecker exporta los enlaces de RPC es /.:/subsys/timechk. El nombre de principal DCE para el servidor es t-checker. El permiso asociado a este servicio es time-check (k).

El permiso para este servidor de autorizaciones externo aparece en Management Console de forma parecida a ésta:

```
Base
  (a) Unir
  (A) Auditoría
  (b) Examinar
  (c) Controlar
  (g) Delegación
  (I) Integridad
  (P) Privacidad
  (T) Atravesar
Genérico
  (k) time-check
Genérico
  (d) Eliminar
  (m) Modificar
  (s) Admin servidor
  (v) Visualizar
NetSEAL
WebSEAL
```

Eliminación de un servidor de autorizaciones externo

Utilice el mandato **ivadmin server delete** para suprimir un servicio de autorizaciones externo registrado. Se utiliza la siguiente sintaxis:

```
ivadmin> server delete /ExternAuthzn/nombre-servidor
```

Donde:

nombre-servidor	Un nombre (o etiqueta) para este servicio de autorizaciones externo. Es el nombre que aparece en la pantalla del espacio de objetos de Management Console.

Por ejemplo:

```
ivadmin> server delete /ExternAuthzn/timechecker
```

Ejemplo 1:

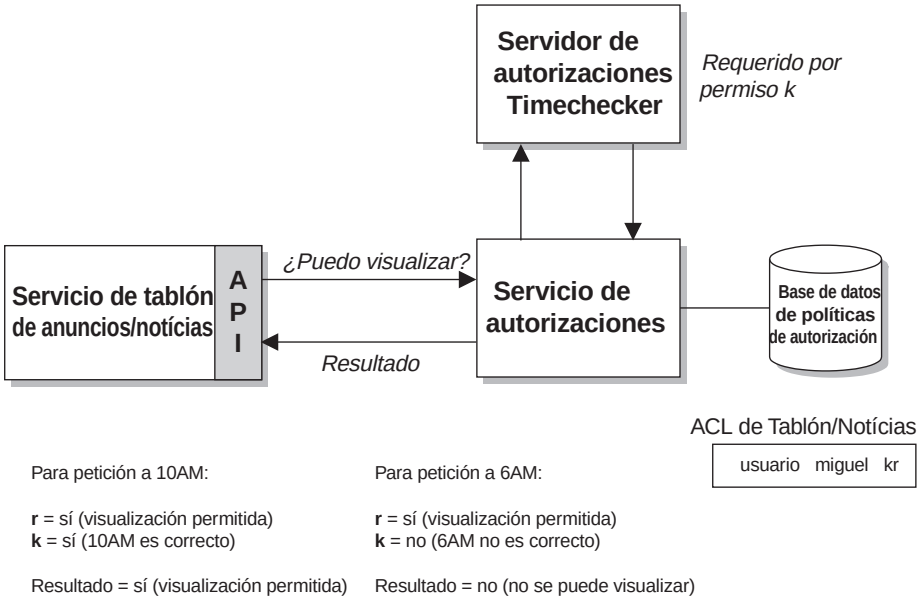
Un servicio de tablón de anuncios y de noticias independiente tiene limitaciones de tiempo en sus operaciones. Los usuarios sólo pueden ver la información proporcionada por este servicio entre las 8 de la mañana y las 5 de la tarde. Se ha escrito un servicio de autorizaciones externo para efectuar una comprobación de la hora en todas las peticiones efectuadas para el servicio del tablón de anuncios y de las noticias.

Utilice el mandato **ivadmin** para configurar el servicio de autorizaciones externo.

La siguiente figura ilustra los posibles supuestos para el proceso de autorizaciones. El usuario debe tener permiso de lectura (r) para ver la información del tablón de

anuncios y de las noticias. La ACL del servicio de noticias también tiene un permiso de comprobación de tiempo (k). El permiso de comprobación de tiempo (k) indica a Policy Director Authorization Service que incluya al servidor de autorizaciones timechecker en la decisión final.

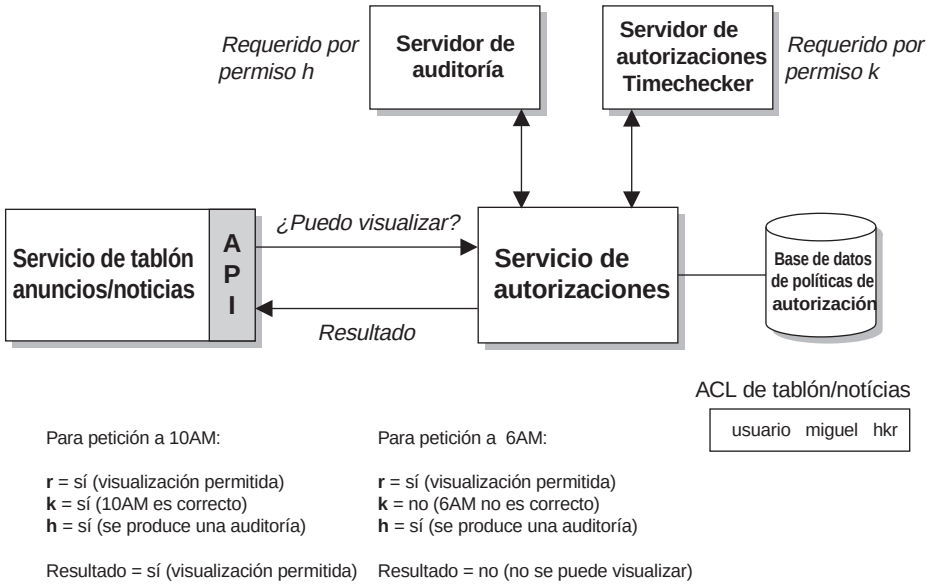
Policy Director basa la decisión de autorización final en la suma de todas las decisiones del servidor de autorizaciones.



Ejemplo 2:

Este ejemplo es igual que el ejemplo 1. Sin embargo, este ejemplo añade un segundo servicio de autorizaciones externo que efectúa una auditoría de la actividad del servicio de tablón de anuncios y de noticias.

Tenga en cuenta que cuando el servicio de autorizaciones Timechecker no permite la visualización, la actividad de auditoría sigue produciéndose. La presencia del permiso **h** requiere la implicación del servidor de autorizaciones de auditoría durante la comprobación de la ACL.



Administración de Management Server

Policy Director Management Server (ivmgrd) gestiona la base de datos de políticas de autorización primaria (maestra). También mantiene la información de ubicaciones de otros servidores WebSEAL y NetSEAL en el dominio seguro. Normalmente, Management Server requiere muy pocas operaciones de administración o configuración. Esta sección indica las tareas de que dispone el administrador.

Definición del número de hebras de notificación de actualizaciones

Management Server (ivmgrd) es el responsable del mantenimiento de la base de datos primaria de políticas de autorización. Security Manager (secmgrd) y Authorization Server (ivacld) son responsables de la creación de réplicas de la base de datos primaria.

Por lo tanto, Management Server es responsable de la sincronización de todas las réplicas de las bases de datos del dominio seguro. Cuando se produce un cambio en la base de datos primaria, las hebras de notificación efectúan el trabajo de anunciar el cambio a todas las réplicas. Después, cada réplica tendrá la responsabilidad de bajar la nueva información de la base de datos primaria.

El archivo de configuración de Management Server, ivmgrd.conf, contiene un parámetro para definir el número máximo de hebras de notificación de actualización. Esta agrupación de hebras permite una notificación simultánea (paralela).

Por ejemplo, para notificar simultáneamente a 30 réplicas un cambio en la base de datos, dé a la agrupación de hebras un valor de 30 como mínimo. SI hay más de 30 réplicas, se producirá otro turno de notificaciones (en este ejemplo, 30 cada vez). Se garantiza que todas las réplicas recibirán la notificación, independientemente del valor de este parámetro.

La finalidad del valor de las hebras de notificación de actualización es anunciar un cambio en base de datos tan rápidamente como sea posible. Generalmente este

valor es igual al número de réplicas existentes. La definición de este valor resulta más ventajosa en lo que se refiere a rendimiento puesto que un solo grupo de hebras realiza rápidamente la tarea de notificación a todas las réplicas a la vez.

El valor por omisión de la agrupación de hebras de notificación de sucesos es:

```
[ivmgrd]
max-notifier-threads = 10
```

Capítulo 12. Registro cronológico y auditoría de la actividad del servidor

Policy Director tiene varias posibilidades de registro cronológico y auditoría. Tiene archivos de anotaciones cronológicas que captan todos los mensajes de error y todos los mensajes de aviso generados tanto por servidores Policy Director Server como DCE Server. También tiene archivos de seguimiento de auditoría que supervisan la actividad de los servidores de Policy Director y DCE.

Este capítulo incluye los siguientes temas:
- Una presentación de las operaciones de registro cronológico y auditoría.
- Una explicación de cada archivo de anotaciones cronológicas.
- Una explicación de cada archivo de auditoría.

Visión general de las operaciones de registro cronológico y auditoría

El contenido de los archivos de anotaciones cronológicas y de seguimiento de auditoría puede ser una útil fuente de información. Utilizando el contenido de los archivos de anotaciones cronológicas y de seguimiento de auditoría puede supervisar la actividad de servidores Policy Director y DCE o resolver los problemas que se presenten.

Archivos de anotaciones cronológicas

Los servidores Policy Director y DCE utilizan archivos de anotaciones cronológicas para almacenar los mensajes de aviso y de error. Todos los archivos de anotaciones cronológicas están en formato de texto.

Policy Director proporciona los siguientes archivos de anotaciones cronológicas:

- Archivo de anotaciones cronológicas de Policy Director Server

  Consulte el apartado “Archivos de anotaciones cronológicas de Policy Director Server” en la página 148.
- Archivo de anotaciones cronológicas de DCE Server

  Consulte el apartado “Archivos de anotaciones cronológicas de DCE Server” en la página 149.
- Mensajes de servicios DCE

  Consulte el apartado “Mensajes de servicios de DCE” en la página 149.
- Archivos de anotaciones cronológicas HTTP estándar

  Consulte el apartado “Registro cronológico de HTTP estándar” en la página 151.

Archivos de seguimiento de auditoría

Los servidores de Policy Director y DCE utilizan archivos de seguimiento de auditoría para almacenar registros de la actividad del servidor. Un *registro* indica la salida de un suceso específico del servidor. Un seguimiento de auditoría es un grupo de varios registros que documentan la actividad del servidor. La mayoría de los archivos de auditoría están en formato ASCII. Los archivos de seguimiento de auditoría de DCE están en formato binario. Para ver estos archivos debe utilizarse el programa de utilidad **dcecp**.

Los siguientes archivos de seguimiento de auditoría proporcionan información sobre sucesos de servidores Policy Director o DCE:

- Estos tres archivos de seguimiento de auditoría de autorizaciones de Policy Director (audit.log):
  - Management Server (ivmgrd)
  - Security Manager (secmgrd)
  - Authorization Server (ivacld)

  Consulte el apartado "Archivos de seguimiento de auditoría de autorizaciones de Policy Director" en la página 154.
- Archivo de seguimiento de auditoría de WebSEAL (wand_audit_log)

  Consulte el apartado "Archivo de seguimiento de auditoría de WebSEAL" en la página 156.
- Archivo de seguimiento de auditoría de Policy Director Management

  Consulte el apartado "Archivo de seguimiento de auditoría de gestión de mandatos de Policy Director" en la página 158.
- Archivos de seguimiento de auditoría de DCE

  Consulte el apartado "Archivos de seguimiento de auditoría de DCE Server" en la página 159.

Convenio para la variable vía-instalación

La variable *vía-instalación* utilizada en todo este capítulo tiene las siguientes interpretaciones, según la plataforma del sistema operativo:
UNIX: `/opt/intraverse/`
Windows:

```
C:\Archivos de programa\IBM\
```

Este nombre de vía de acceso no puede cambiarse en UNIX porque es fijo.

La plataforma Windows permite definir la *vía-instalación* durante la instalación del software de Policy Director.

Archivos de anotaciones cronológicas de Policy Director Server

Cada servidor de Policy Director genera dinámicamente mensajes de aviso y de error que se dirigen a errores estándar y que, a continuación, se redirigen a archivos de anotaciones cronológicas específicos.

Servidor	Proceso	Ubicación archivo anotaciones
Management Server	**ivmgrd**	Definida en ivmgrd.conf: arch-anot=*vía-instalación*/ivmgrd/log/ivmgrd.log
Security Manager	**secmgrd**	Definida en secmgrd.conf: arch-anot=*vía-instalación*/secmgr/log/secmgrd.log
Authorization Server	**ivacld**	Definida in ivacld.conf: arch-anot=*vía-instalación*/ivacld/log/ivacld.log
Directory Services Broker	**nsid**	*vía-instalación*/broker/nsid.log

Habilitación e inhabilitación de archivos de anotaciones cronológicas

Policy Director habilita el registro cronológico cuando en el archivo de configuración hay un archivo de anotaciones cronológicas definido.

Ejemplo secmgrd.log

El archivo secmgrd.log tiene un contenido parecido al siguiente:

```
1998-09-22-21:56:36.898-04:00I----- secmgrd FATAL ivc general
exec.c 344 0x00000006
Caught signal (15)
1998-09-22-21:56:37.309-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1039 0x00000001
Could not unexport bindings from name service
(/.:/subsys/ibm/secmgr/server/sun,0x16c9a093
1998-09-22-21:56:37.354-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1048 0x00000001
Could not unregister RPC endpoints (0x16c9a042)
```

Archivos de anotaciones cronológicas de DCE Server

Cada DCE Server genera dinámicamente mensajes de aviso y de error que se dirigen a errores estándar y que, a continuación, se redirigen a archivos de anotaciones cronológicas específicos. Estos archivos de anotaciones cronológicas pueden ser útiles fuentes de información para buscar y corregir un problema.

Los archivos de anotaciones cronológicas de DCE Server incluyen:

Security Server:

UNIX: `/opt/dcelocal/var/security/secd.log`

Windows: `\Archivos de programa\IBM\dcelocal\var\security\secd.log`

DCE Server:

UNIX: `/opt/dcelocal/var/dced/dced.log`

Windows: `\Archivos de programa\IBM\dcelocal\var\dced\dced.log`

Mensajes de servicios de DCE

El archivo de rutas controla los mensajes de servicios de DCE:

UNIX: `/opt/dcelocal/var/svc/routing`

Windows: `\Archivos de programa\IBM\NetSEAT\var\svc\routing`

Nota: En sistemas Windows, la vía de instalación puede configurarse durante la instalación: `\Archivos de programa\IBM\NetSEAT\`. La variable de entorno (%NETSEAT%) se resuelve en la vía de acceso configurada.

Entradas por omisión en el archivo de rutas

Las entradas de este archivo de configuración determinan el tipo de información que se anota cronológicamente. El archivo *de rutas* incluye las siguientes entradas por omisión:

UNIX:
```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
```

Windows:
```
FATAL:STDERR:-;FILE:%NETSEAT%\var\svc\fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%\var\svc\error.log
WARNING:STDERR:-;FILE:%NETSEAT%\var\svc\warning.log
```

Los mensajes NOTICE proporcionan más información sobre la actividad del servidor. Por omisión, Policy Director no habilita mensajes NOTICE (no hay ninguna entrada en el archivo),

Para habilitar los mensajes NOTICE (y dirigirlos a errores estándar), añada la siguiente nueva línea NOTICE al final del archivo de rutas:

UNIX:
```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
NOTICE:STDERR:-;FILE:/opt/dcelocal/var/svc/notice.log
```

Windows:
```
FATAL:STDERR:-;FILE:%NETSEAT%\var\svc\fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%\var\svc\error.log
WARNING:STDERR:-;FILE:%NETSEAT%\var\svc\warning.log
NOTICE:STDERR:-;FILE:%NETSEAT%\var\svc\notice.log
```

Modalidad de depuración para dirigir mensajes a la salida estándar

Normalmente, Policy Director redirige los mensajes de aviso y de error, incluidos los mensajes NOTICE, a los archivos de anotaciones cronológicas adecuados.

Para dirigir estos mensajes a una salida estándar (terminal), utilice la opción de mandato **-debug** cuando inicie el servidor. Esta opción hace que el servidor se ejecute en primer plano (es decir, que el servidor no se coloca a sí mismo como daemon). Policy Director escribe mensajes de aviso y de error en la salida estándar.

Por ejemplo, para iniciar Security Manager (secmgrd) en modalidad de depuración, utilice el siguiente mandato:

```
# /opt/intraverse/secmgr/bin/secmgrd -debug
```

También puede utilizar el mandato **tee** de UNIX para capturar la salida del servidor en un solo archivo.

El siguiente ejemplo ilustra el inicio de Policy Director Security Manager en esta modalidad:

```
# secmgrd -debug 2>&1 | tee /tmp/secmgrd.log
```

Notas sobre depuración

Cuando efectúe una depuración, tenga en cuenta lo siguiente:

1. Cuando termine de reunir la información sobre la actividad del servidor, asegúrese de restaurar el archivo de rutas a su condición normal. Suprima la entrada NOTICE. NOTICE genera una gran cantidad de información que puede acumularse rápidamente.
2. Puede utilizar **Control + c** para interrumpir un proceso servidor iniciado en modalidad de depuración. El proceso servidor se cierra correctamente y sale.

Registro cronológico de HTTP estándar

Policy Director WebSEAL Server también mantiene tres archivos de anotaciones cronológicas convencionales de HTTP que registran la actividad en vez de registrar mensajes:

wand_request_log
Consulte el apartado “Visualización de wand_request_log” en la página 153.

wand_agent_log
Consulte el apartado “Visualización de wand_agent_log” en la página 153.

wand_referer_log
Consulte el apartado “Visualización de wand_referer_log” en la página 153.

Por omisión, Policy Director mantiene estos archivos de anotaciones cronológicas bajo el siguiente directorio:

UNIX: `/opt/intraverse/www/log`

Windows: `\Archivos de programa\IBM\Policy Director\www\log`

Configuración del registro cronológico de HTTP estándar

La sección `[wand]` del archivo de configuración iv.conf contiene parámetros para configurar el registro cronológico de HTTP estándar.

La siguiente tabla ilustra las relaciones entre los archivos de anotaciones cronológicas de HTTP y los parámetros del archivo de configuración:

Archivos de anotaciones cronológicas	Parámetro de ubicación	Habilitar/Inhabilitar parámetro (= yes o no)
wand_request_log	reqlog =	logreqs =
wand_referer_log	reflog =	logrefs =
wand_agent_log	agentlog =	logagents =

Por ejemplo, la entrada de iv.conf correspondiente a la ubicación por omisión de **wand_request_log** aparece como sigue:

```
reqlog = log/wand_request_log
```

El directorio root para esta ubicación es:

UNIX: `/opt/intraverse/www/`

Windows: `\Archivos de programa\IBM\Policy Director\www\`

Habilitación e inhabilitación del registro cronológico de HTTP

Por omisión, Policy Director habilita el registro cronológico de todo el HTTP:

```
[wand]
logreqs = yes
logrefs = yes
logagents = yes
```

Para inhabilitar el registro cronológico, indique:

```
<enable-parameter> = no
```

Especificación de tipo de indicación de la hora

Puede decidir tener indicaciones de la hora en cada anotación cronológica registrada con la Hora Media de Greenwich (GMT) en vez de con el huso horario local. Por omisión, Policy Director utiliza el huso horario local:

```
[wand]
loggmttime = no
```

Para utilizar indicaciones de la hora GMT, indique:

```
loggmttime = yes
```

Nota: Puede ser conveniente conservar todos los archivos de anotaciones cronológicas en tiempos sincronizados para que sea más fácil la lectura de los archivos de anotaciones cronológicas y de auditoría procedentes de todos los productos relacionados con la seguridad.

Especificación del tamaño máximo del archivo de anotaciones cronológicas

El tamaño máximo de cada archivo de anotaciones cronológicas de HTTP se define por omisión:

```
[wand]
logsize = 2000000
```

Policy Director hace una copia de seguridad del archivo de anotaciones cronológicas cuando éste llega a su tamaño máximo.

Recuerde que este parámetro también afecta al archivo de seguimiento de auditoría de Policy Director **wand_audit_log**.

Compruebe frecuentemente el tamaño de los archivos de anotaciones cronológicas para asegurarse de que no están creciendo demasiado y ocupando demasiado espacio. Archive periódicamente los archivos de anotaciones cronológicas cuando efectúe el mantenimiento normal del sistema.

Utilización del formato común de anotaciones cronológicas de HTTP

Todas las respuestas (satisfactorias o de error) que se devuelven a Policy Director Server se registran con una entrada de una línea con el siguiente formato común de anotaciones cronológicas de HTTP:

```
sistpral - usuaut [fecha] petic estado bytes
```

Donde:

sistpral Especifica la dirección IP (Internet Protocol) de la máquina solicitante.

usuaut Toma el valor de la cabecera **From:** de la petición de HTTP recibida. Además, este campo también transmite una petición de RPC segura al darle el valor dce-rpc. Este campo está en blanco para un usuario no autentificado.

fecha Especifica la fecha y la hora de la petición.

petic Especifica la primera línea de la petición tal como llegó del cliente.

estado Especifica el código de estado de HTTP devuelto a la máquina solicitante.

bytes Especifica el número de bytes devueltos a la máquina solicitante. En otras palabras, se transfiere la longitud del contenido del documento.

Visualización de wand_request_log

wand_request_log registra el registro cronológico estándar de peticiones HTTP. Los registros cronológicos estándar incluyen, por ejemplo, información sobre los URL que se hayan solicitado e información sobre el cliente (por ejemplo, la dirección IP) que efectuó la petición.

El archivo wand_request_log tiene un contenido similar al siguiente:

```
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:33 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:47 EDT]
  "GET /icons HTTP/1.0" 302 93
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:59 EDT]
  "GET /icons/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue,  23 Apr 1996 17:24:04 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:24:11 EDT]
  "GET /~smith/ HTTP/1.0" 403 77
dce-rpc - - [Tue, 23 Apr 1996 17:24:51 EDT]
  "GET / HTTP/1.0" 200 919
```

Visualización de wand_agent_log

wand_agent_log registra el contenido de la cabecera `User_Agent:` de la petición HTTP. Esta anotación cronológica contiene, para cada petición, cierta información sobre el navegador cliente como, por ejemplo, la arquitectura o el número de versión.

El siguiente ejemplo es una versión de muestra de un archivo wand_agent_log:

```
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
```

Visualización de wand_referer_log

wand_referer_log registra la cabecera de la petición HTTP. Para cada petición, la anotación cronológica registra el documento que contenía el enlace con el documento solicitado.

La anotación cronológica tiene el siguiente formato:

```
referer -> objeto
```

Esta información resulta útil para efectuar el seguimiento de enlaces externos con documentos del espacio de la Web. La anotación cronológica muestra que el origen indicado por `referer` contiene un enlace con un *objeto* de página. Esta anotación cronológica permite efectuar el seguimiento de enlaces caducados y averiguar quién está creando enlaces con los documentos.

El siguiente es un ejemplo de una versión de muestra de un archivo wand_referer_log:

```
http://manuel/maybam/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
```

Archivos de seguimiento de auditoría de autorizaciones de Policy Director

Cada servidor de Policy Director puede capturar sucesos de auditoría siempre que se produce una actividad auditable relacionada con la seguridad. Policy Director guarda los sucesos de auditoría como registros de auditoría que documentan la actividad específica de ese servidor. Varios registros de auditoría forman un archivo de seguimiento de auditoría.

La siguiente tabla ilustra la relación entre cada servidor de Policy Director y el archivo de seguimiento de auditoría relacionado con él:

Servidor	Proceso	Archivo de auditoría de autorización
Management Server	**ivmgrd**	Defined in ivmgrd.conf: audit-file= *vía-instalación*/ivmgrd/log/audit.log
Security Manager	**secmgrd**	Defined in secmgrd.conf: authzn-audit-file= *vía-instalación*/secmgr/log/audit.log
Authorization Server	**ivacld**	Defined in ivacld.conf: audit-file= *vía-instalación*/ivacld/log/audit.log

Policy Director graba la información de autorización en el archivo de seguimiento de auditoría adecuado siempre que se ha definido el permiso de auditoría (A) para un usuario o grupo en una ACL. Los registros de auditoría resultantes incluyen todos los intentos de acceso, incluidos los errores de autorización.

Administración de seguimiento de auditoría

El permiso de auditoría audit (A) en una entrada de ACL activa la información de actividad de registro de los archivos de seguimiento de auditoría de autorización de Policy Director. La activación de la auditoría a través del permiso de auditoría (A) es fácil de llevar a cabo.

Las siguientes condiciones se aplican a la gestión de archivos de seguimiento de auditoría de autorizaciones:

- El objeto al que se une la ACL determina cuál de los tres archivos audit.log recoge los datos.

  Por ejemplo, se puede unir la ACL que contiene el permiso de auditoría (A) a una o más entradas del objeto /Management del espacio de nombres de objetos protegidos. Si se hace así, los datos se reunirán en el archivo audit.log de Management Server (ivmgrd). Management Server controla la base de datos de políticas de autorización (ACL) y la réplica de la base de datos (Replica).
- Cuando se define el permiso de auditoría en la entrada de ACL adecuada, sólo se reúne información de actividad de usuarios, de grupos o de ambos.

Por ejemplo, se puede proporcionar a la entrada no autentificada el permiso de auditoría (A) en una ACL que esté unida a un objeto de página HTML. Con este permiso, el archivo audit.log de Security Manager recogerá información de todos los intentos de acceder al objeto en los que no se ha concedido la autorización.

Ejemplo: La siguiente ACL representa la ACL default-webseal. La entrada de usuario cell_admin o la entrada authenticated tiene definidos permisos de auditoría (A).

```
usuario cell_admin                aAbcTdmlrx
grupo iv-admin                    abdTdmlrx
grupo servidores-ivmgrd           Tl
grupo servidores-webseal)         gTdmlrx
autentificado por cualquiera      Tr
no autentificado                  ATr
```

Una ACL unida al objeto /WebSEAL indica que está unida al root de la región WebSEAL del espacio de nombres de objetos protegidos. Si está unida, Policy Director registrará la actividad que implica al servidor Security Manager (WebSEAL y NetSEAL) en el archivo audit.log de Security Manager.

Es posible que el espacio de nombres de WebSEAL no contenga ninguna otra ACL explícita que modifique las condiciones del permiso. Si no hay ninguna otra ACL explícita, se llevará a cabo la auditoría para todas las peticiones para cualquier objeto del espacio de la Web.

El archivo de seguimiento de auditoría sólo registra la actividad iniciada por el usuario cell_admin y todos los intentos de acceso no autentificados.

Una ACL explícita unida a un objeto que se encuentre en algún lugar por debajo del objeto /WebSEAL romperá la cadena de valores heredados de la ACL. Es posible que las entradas de esta ACL explícita no contengan ningún permiso de auditoría. Si las entradas no contienen ningún permiso de auditoría, no se generará ningún seguimiento de auditoría para ese objeto ni para ningún otro objeto situado por debajo de este punto.

Nota: Acuérdese de añadir el permiso de auditoría a las entradas pertinentes de cualquier ACL que esté uniendo explícitamente a los objetos que se encuentren por debajo del objeto /WebSEAL.

Ejemplo de archivo de seguimiento de auditoría de Management Server

Un archivo de seguimiento de auditoría de Management Server tiene un contenido parecido al siguiente:

```
START RECORD
  Protected object: /WebSEAL
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorized
END RECORD

START RECORD
  Protected object: /WebSEAL/sun
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
```

```
  quality of protection: none    result: authorize
END RECORD

START RECORD
  Protected object: /WebSEAL/sun/icons
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD

START RECORD
  Protected object: /WebSEAL
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
```

Archivo de seguimiento de auditoría de WebSEAL

También se puede supervisar la actividad de un servidor de Policy Director WebSEAL. Policy Director guarda los sucesos de auditoría como registros de auditoría que documentan la actividad específica de ese servidor. Varios registros de auditoría forman un archivo de seguimiento de auditoría.

Auditoría de WebSEAL

Los parámetros para configurar los archivos de seguimiento de auditoría de WebSEAL se encuentran en la sección [wand] del archivo de configuración iv.conf.

La siguiente tabla ilustra la relación entre WebSEAL y el archivo de seguimiento de auditoría:

Servidor	Archivo de auditoría
WebSEAL	Definido en iv.conf: auditlog= *vía-instalación*/www/log/wand_audit_log

Habilitación e inhabilitación de la auditoría de WebSEAL

Por omisión, la auditoría de WebSEAL está inhabilitada:

```
[wand]
logaudit = no
```

Para activar la auditoría, indique:

```
logaudit = yes
```

Nota: No debe haber ningún espacio en blanco después de yes o no cuando se edita este parámetro en el archivo de configuración iv.conf.

Especificación de la ubicación del archivo de anotaciones cronológicas

La ubicación por omisión del archivo de auditoría de WebSEAL es:

```
[wand]
auditlog = log/wand-audit-log
```

Especificación del tamaño máximo del archivo de anotaciones cronológicas

Policy Director define un tamaño máximo para el archivo de anotaciones cronológicas de auditoría:

```
[wand]
logsize = 2000000
```

Cuando una anotación cronológica alcanza este tamaño, Policy Director hace una copia de seguridad del archivo de anotaciones cronológicas. Entonces, un archivo de anotaciones cronológicas de auditoría vacío se convierte en el archivo de anotaciones cronológicas de auditoría por omisión. Recuerde que este parámetro también afecta a los siguientes archivos de anotaciones cronológicas de HTTP:

- wand_request_log
- wand_referer_log
- wand_agent_log

Sintaxis del archivo de seguimiento de auditoría de WebSEAL

Todas las respuestas satisfactorias o de error que devuelve WebSEAL Server se registran con una entrada de una línea en el siguiente formato:

```
sistpral tipo_llamada uri cód_estado_iv [fecha] uuid lista_uuid_grupo
```

sistpral (y punto de terminación)	Información de punto final y dirección IP del sistema principal remoto. Si no hay información de punto de terminación, se visualiza [-].
tipo_llamada	0 para una conexión TCP, 1 para UNAUTH RPC y 2 para AUTH RPC
uri	Indicador de petición universal para la petición.
cód_estado_iv	Código de estado de este subconjunto Policy Director del servicio de auditoría estándar.
fecha	Fecha y hora de la petición.
uuid (indicado con el indicador **-p**)	UUID del cliente. Si no hay información del UUID, no se visualiza nada.
lista_uuid_grupo (se indica con el indicador **-g**)	Lista de UUID de grupo. Si no hay información del UUID de grupo, no se visualiza nada.

Ejemplo de contenido del archivo de seguimiento de auditoría

Un archivo de seguimiento de auditoría tiene un contenido parecido al siguiente:

```
204.30.81.188[33380] 2 /audit_report.html 0x18a2141a
[21/Aug/1997:14:36:23 -0700]
-p 00000064-0f4c-21d1-9300-00c078500371
-g 0000000c-0f4c-21d1-9301-00c078500371
-g 0000044c-0f4c-21d1-8601-00c078500371
-g 0000044d-0f4c-21d1-8601-00c078500371
```

Detalles:

sistpral:	204.30.81.188
punto de terminación:	[33380]
tipo_llamada:	2
uri:	/audit_report.html
cód_estado_iv:	0x18a2141a
fecha:	[21/Aug/1997:14:36:23 -0700]
uuid:	-p 00000064-0f4c-21d1-9300-00c078500371

lista_uuid_grupo:	-g 0000000c-0f4c-21d1-9301-00c078500371 -g 0000044c-0f4c-21d1-8601-00c078500371 -g 0000044d-0f4c-21d1-8601-00c078500371

Nota: Es posible que la cadena de caracteres que forma el URI aparezca únicamente como un guión. Esta condición puede deberse a una terminación prematura de la petición o a un error en la cadena de caracteres de la petición.

Archivo de seguimiento de auditoría de gestión de mandatos de Policy Director

Cada servidor de Policy Director puede capturar sucesos de auditoría siempre que se produce una actividad auditable relacionada con la gestión. Policy Director guarda los sucesos de auditoría como registros de auditoría que documentan la actividad específica de ese servidor. Varios registros de auditoría forman un archivo de seguimiento de auditoría.

La siguiente tabla ilustra la relación entre cada servidor de Policy Director y el archivo de seguimiento de auditoría relacionado con él:

Servidor	Proceso	Archivo de auditoría de gestión
Management Server	**ivmgrd**	Definido en ivmgrd.conf: mgr-audit-file= *vía-instalación*/ivmgrd/log/mgraudit.log

Entre las responsabilidades de Management Server se incluye el mantenimiento de la base de datos primaria de políticas de autorización.

Esta base de datos incluye la descripción del espacio de nombres de objetos protegidos correspondiente al dominio seguro, las plantillas de políticas ACL e indica dónde se han unido las ACL a objetos.

Esta base de datos incluye:

- La descripción del espacio de nombres de objetos protegidos correspondiente al dominio seguro.
- Las plantillas de políticas de ACL.
- La información que indica dónde están unidas las ACL a objetos.

Se pueden capturar todos los sucesos de mandatos desde Management Console o utilizando el programa de utilidad **ivadmin** en el archivo mgraudit.log.

Contenido del registro de auditoría

Los registros de auditoría se graban en registros identificados con el sistema de corchetes tipo XML. Un suceso de auditoría captura la siguiente información:

ID originador
Se deriva del descriptor de contexto del cliente de RPC entrante que se imprime como una lista de UUID o de la cadena de caracteres `unauthenticated`, según corresponda.

Indicador: `P`

ID de suceso
Número que identifica de forma exclusiva a un mandato de gestión definido en la cabecera ../ivmgrd/cmdConst.h.

Indicador: I

Salida de mandato
Número que corresponde al código de estado devuelto a quien efectúa la llamada.

Identificador: O

Indicación de la hora
Registro que indica la hora en que terminó el mandato con el mismo formato utilizado actualmente por la auditoría de bit de ACL.

Indicador: D

Vector de argumento de mandato
Representación de los argumentos de entrada del mandato.

Indicadores: V y A

Ejemplo de archivo de seguimiento de auditoría de Management Server

Un archivo de seguimiento de auditoría de Management Server tiene un contenido parecido al siguiente:

```
<E><D>Fri May 30 00:00:00 1999<\D><I>3008</I><O>0</O><P>[1]
069d9fb6-943e-11cd-a35c-0000c08adf56</P><V><A> argumento
1</A><A>argumento 2</A></V></E>
```

Archivos de seguimiento de auditoría de DCE Server

Los siguientes archivos de seguimiento de auditoría de DCE Server utilizan el servicio de auditoría de DCE. Los archivos tienen un formato binario. Para visualizar los archivos debe utilizarse el programa de utilidad **dcecp**.

1. Seguimiento de auditoría de DCE Security Service (secd)
   /opt/dcelocal/var/security/sec_audit_trail
   /opt/dcelocal/var/security/sec_audit_trail.md_index
2. Seguimiento de auditoría de DCE Audit Service (auditd)
   /opt/dcelocal/var/security/central_trail
   /opt/dcelocal/var/security/central_trail.md_index
3. Seguimiento de auditoría de DCE Time Service (dtsd)
   /opt/dcelocal/var/security/dts_aud_trail
   /opt/dcelocal/var/security/dts_aud_trail.md_index

Ejemplo de sec_audit_trail

```
dcecp> login cell_admin
Enter Password:
dcecp>

--- Event Record number 261 ---
o Event Information:
   - Event Number:          0x101 /* 257 */
   - Event Name:          AS_Request
   - Event Outcome:          success
o Server:          /.:/hosts/eggman
o Client:          /.../eggman_cell/cell_admin
o Number of groups:          0
o Authorization Status:          Authorized with a name
o Date and Time recorded: 1998-10-20-10:42:56.248-04:00I-----
--- End of Event record number 261 ---
```

Capítulo 13. WebSEAL: Configuración de la autentificación

Policy Director WebSEAL tiene soporte para LDAP, Kerberos y mecanismos de autentificación de claves públicas y privadas. Un importante derivado del proceso de autentificación es la adquisición de credenciales de usuario. Las credenciales de usuario se utilizan durante la autorización de peticiones para acceder a recursos protegidos.

Este capítulo incluye los siguientes temas:

Visión general de la autentificación de WebSEAL

Esta sección trata del soporte de WebSEAL para:

- Una comunicación segura a través del protocolo SSL.
- Mecanismos de autentificación.
- Métodos para proporcionar información de identidad.
- Ampliación de los mecanismos de autentificación estándar.

Soporte para SSL

WebSEAL tiene soporte para comunicaciones seguras a través del protocolo Secure Socket Layer (SSL). Estas secciones tratan de la comunicación segura a través del protocolo SSL:

- "Configuración de WebSEAL para SSL" en la página 162.
- "Creación de un certificado del área del servidor para WebSEAL" en la página 165.

Mecanismos de autentificación

La autentificación es el proceso en el que se identifica a un individuo que intenta iniciar la sesión con un dominio seguro. WebSEAL tiene soporte para los siguientes mecanismos de autentificación.

- Clave secreta LDAP
- Kerberos Versión 5
- Claves pública y privada

Información de identificación del cliente

El proceso de autentificación requiere que el cliente proporcione algún tipo de información de identidad durante el inicio de sesión. WebSEAL tiene soporte para los siguientes métodos de provisión de información de identidad:

1. Nombre de usuario y contraseña (utilizados por LDAP y Kerberos)
   - Autentificación básica
   - Inicio de sesión basado en formularios

   Consulte el apartado “Métodos de autentificación de nombre de usuario y de contraseña” en la página 171.
2. Certificado X.509 del área del cliente (utilizado por las claves pública/privada)

   Consulte el apartado “Método de autentificación de certificado X.509” en la página 175.

Adquisición de credenciales

Puede utilizar un servicio de adquisición de credenciales para ampliar los mecanismos de autentificación estándar soportados por WebSEAL. Consulte el apartado “Configuración de Policy Director Credentials Acquisition Service” en la página 177.

Configuración de WebSEAL para SSL

El servidor Policy Director WebSEAL tiene soporte para comunicaciones seguras con navegadores clientes que utilizan el protocolo Secure Socket Layer (SSL).

Cuando se utiliza este protocolo, los clientes pueden utilizar uno de dos métodos para pasar la información de identidad a WebSEAL:

- Nombre de usuario y contraseña
- Certificado digital X.509 del área del cliente

En ambas modalidades, WebSEAL se autentifica a sí mismo ante el cliente utilizando su certificado digital del área del servidor. Una autoridad de certificación (Certificate Authority, CA) emite el certificado X.509. Policy Director almacena el certificado y la clave privada asociada en un archivo con formato PEM o con formato PKCS#12.

Cuando se utiliza el formato PEM, Policy Director almacena en archivos separados la clave privada y la clave pública firmada del servidor. Cuando se utiliza el formato PKCS#12, los pares de claves generados y almacenados residen juntos en un solo archivo.

Es aconsejable que el nombre común (CN) del certificado del servidor sea igual que el nombre completo del sistema principal del WebSEAL Server.

Aunque no es necesario, muchos navegadores clientes comprueban si una autoridad de certificación ha emitido el certificado del servidor. La comprobación se efectúa a través de la base de datos de certificados root de CA. Si el firmante del certificado no coincide con una de las entradas de la base de datos de certificados root de CA, se visualizará un mensaje de aviso. Será responsabilidad del usuario el aceptar o rechazar la conexión con ese servidor.

En el apartado “Creación de un certificado del área del servidor para WebSEAL” en la página 165 encontrará la información completa para obtener e instalar un certificado X.509 del área del servidor para WebSEAL.

En la modalidad de certificados del área del cliente, WebSEAL se autentifica a sí mismo ante el cliente utilizando su certificado digital del área del servidor, como se explicaba anteriormente. Además, WebSEAL requiere un certificado root X.509

de CA procedente de una autoridad de certificación (CA) que pueda validar el certificado del área del cliente. Una petición de cliente, efectuada utilizando un certificado del área del cliente, proporciona una autentificación mutua fiable.

Utilización de certificados del área del servidor y de certificados root de CA

Un certificado X.509 del área del servidor identifica un WebSEAL Server ante un cliente. Policy Director almacena certificados del área del servidor en formato PEM o PKCS#12, como se indica a continuación:

- Formato PEM—archivos separados que almacenan la clave privada y la clave pública firmada
- Formato PKCS#12—un solo archivo que contiene la clave privada y la clave pública del servidor.

Nota: WebSEAL sólo puede contener y soportar un certificado de servidor. WebSEAL no tiene soporte para varias instancias de servidores Web lógicos en la misma máquina.

Un *certificado root de CA* identifica a una autoridad de certificación (CA) específica. WebSEAL necesita el certificado root de CA para validar un certificado del área del cliente. WebSEAL puede mantener una lista de certificados root de CA en formato PEM, formato PKCS#12 o una combinación de los dos, como puede verse a continuación:

- Formato PEM—acumula certificados root en un solo archivo
- Formato PKCS#12—almacena certificados root como archivos separados en un directorio común

Almacenamiento de certificados

El archivo de configuración secmgrd.conf define los parámetros de almacenamiento de certificados. Los parámetros son distintos, dependiendo de si el parámetro se utiliza para UNIX o para Windows.

Parámetro	Descripción
Para UNIX: `ca-directory = /opt/intraverse/lib/certs` **Para Windows:** `ca-directory = C:\Archivos de programa\ibm\Policy Director\lib\certs`	
	Directorio base para almacenamiento de certificados.
Para UNIX: `ca-cert-file = /lib/certs/cacert.pem` **Para Windows:** `ca-cert-file = C:\Archivos de programa\ibm\Policy Director\lib\certs\cacert.pem`	
	El certificado root X.509 de CA de una autoridad de certificación reconocida, en formato PEM. WebSEAL acepta certificados X.509 del área del cliente de una CA fiable en formato PEM. Pueden añadirse a este archivo certificados root de otros CA.
Para UNIX: `ca-cert-p12-dir = /opt/intraverse/lib/certs/ca_p12` **Para Windows:** `ca-cert-p12-dir = C:\Archivos de programa\ibm\Policy Director\lib\certs\ca_p12`	
	El directorio designado para un archivo que contiene el certificado root X.509 de una autoridad de certificación reconocida, en formato PKCS#12. WebSEAL acepta certificados X.509 del área del cliente de una CA fiable en formato PKCS#12. En este directorio pueden almacenarse certificados root de otras CA.

Para UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.pem` **Para Windows:** `certificate-file = C:\Archivos de programa\ibm\Policy Director\lib\certs\svrcert.pem`	
	El certificado X.509 del servidor procedente de la CA, en formato PEM. Este certificado se presenta a los clientes SSL. El ejemplo de certificado que contiene este archivo debe cambiarse por un certificado legitimado procedente de una CA fiable.
Para UNIX: `key-file = /opt/intraverse/lib/certs/srvkey.pem` **Para Windows:** `key-file = C:\Archivos de programa\ibm\Policy Director\lib\certs\srvkey.pem`	
	La clave privada del servidor, en formato PEM. La clave de ejemplo que contiene este archivo en la instalación debe cambiarse por una clave legitimada generada por el usuario.
Para UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.p12` **Para Windows:** `certificate-file = C:\Archivo de programas\ibm\Policy Director\lib\certs\svrcert.p12`	
	El certificado X.509 del servidor procedente de la CA, en formato PKCS#12. El archivo incluye la clave privada. El certificado y la clave de ejemplo que contiene este archivo deben cambiarse por un certificado y una clave legitimados procedentes de una CA fiable.
Para UNIX y Windows: **clave de contraseña =** *frase de contraseña*	
	La contraseña de clave (*frase de contraseña*) utilizada para desbloquear el archivo de la clave privada.

Configuración de la gestión de certificados

La sección `[wand]` del archivo de configuración iv.conf contiene el parámetro para la gestión de certificados X.509 del área del cliente. Se puede indicar cómo debe gestionar WebSEAL los certificados X.509 del área del cliente definiendo el parámetro **verify-clients** (verificar clientes). Los valores permitidos para verify-clients son los siguientes:

Valor	Descripción
never (nunca)	No solicitar certificados X.509 de clientes. Se obliga a los clientes a que accedan utilizando el nombre de usuario y la contraseña.
optional (opcional)	Solicitar a los clientes un certificado X.509 y utilizar la autentificación basada en certificados, si existe. Cuando el cliente no presenta un certificado, obligar a los clientes a utilizar la autentificación básica.
required (obligatorio)	Pedir a los clientes un certificado X.509 y utilizar la autentificación basada en certificados. Cuando el cliente no presenta un certificado, no permitir la conexión.

Por omisión, WebSEAL no solicita certificados del área del cliente:

```
[wand]
verify-clients = never
```

Definición del tiempo de espera en antememoria de sesión SSL

La sección `[ssl]` del archivo de configuración secmgrd.conf contiene el parámetro para definir el tiempo de espera estático de antememoria de sesión SSL.

WebSEAL coloca internamente en la antememoria la información sobre credenciales. Este parámetro de caducidad de credenciales indica el periodo de tiempo que la información sobre credenciales de autorización permanece en la memoria de WebSEAL.

Este parámetro no indica un tiempo de espera por inactividad. El valor se correlaciona con un “tiempo de vida de credencial” en vez de con un ”tiempo excedido de credencial”. Su finalidad es mejorar la seguridad forzando al usuario a volver a autentificarse cuando Policy Director alcanza el límite de tiempo de espera especificado.

El tiempo de espera en la antememoria (en segundos) por omisión es:

```
[ssl]
ssl-cache-timeout = 3600
```

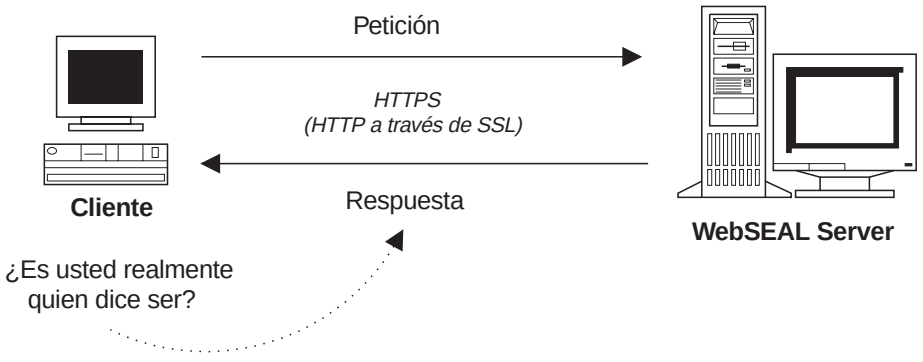
Ajuste este valor para equilibrar el rendimiento del servidor a conveniencia del usuario, dependiendo del volumen de peticiones SSL que debe gestionar el servidor.

Nota: Algunos navegadores ejecutan una renegociación automática de la sesión. Si su navegador es de este tipo, este parámetro no tendrá efectividad.

Creación de un certificado del área del servidor para WebSEAL

Puede configurar un Policy Director WebSEAL Server para permitir que clientes habilitados para SSL verifiquen la autenticidad del servidor. Esta sección explica las tareas administrativas necesarias para crear certificados del área del servidor en formato PEM.

La tarea implica específicamente el registro con una CA válida o con un producto de generación de certificados controlado internamente. El registro debe obtener un certificado del servidor local que permita a Policy Director aceptar y responder adecuadamente a las peticiones de los navegadores habilitados para SSL.

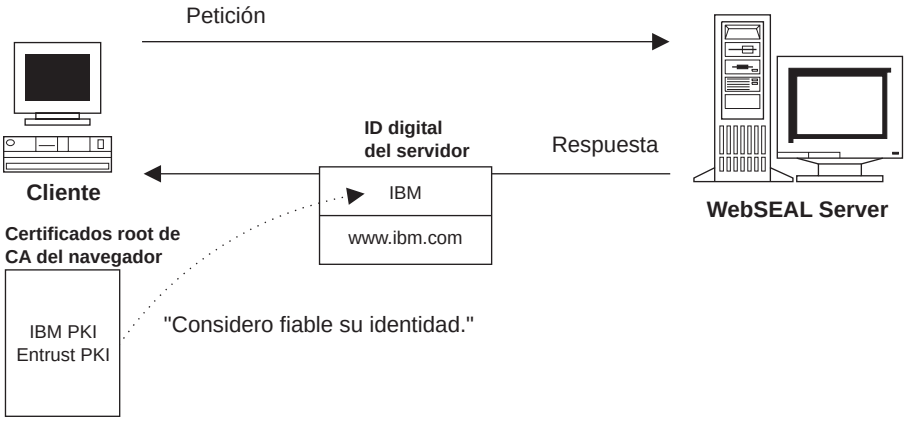


Asegurar una comunicación segura a través de SSL

Policy Director WebSEAL Server tiene soporte para la autentificación de clientes utilizando HTTP a través de SSL (HTTPS). WebSEAL debe tener instalado un certificado X.509 público del área del servidor que utilizará para responder a los clientes. El certificado X.509 prueba al cliente que la respuesta de WebSEAL procede de un servidor permitido.

Para que la comunicación SSL sea segura a través de Internet, el navegador debe autentificar el servidor. El navegador efectúa la autentificación comprobando si el certificado de clave pública tiene un certificado root de CA coincidente. Los certificados coincidentes de CA pueden estar enlazados con el navegador o el navegador puede adquirirlos.

Un certificado de servidor permitido, firmado por una CA, evita la posibilidad de suplantación de personalidad.



WebSEAL se envía con una muestra de certificado de servidor firmada por una autoridad de certificación IBM de ejemplo. Esta muestra de certificado permite a WebSEAL responder a la petición de un navegador habilitado para SSL. Sin embargo, el navegador no podrá verificar el ejemplo de certificado porque éste no contiene ningún certificado de root de CA de IBM. Por lo tanto, la comunicación que ofrece no es fiable ni segura.

Para asegurar una comunicación segura a través de SSL, es importante registrarse para un certificado de servidor local de una autoridad de certificación fiable. Puede obtener un certificado de servidor local de una CA reconocida o generar un certificado “propio” utilizando software como, por ejemplo, IBM SecureWay Trust Authority.

La configuración de Policy Director para establecer comunicaciones a través de SSL implica las siguientes tareas:

- “Generación de una clave pública y una clave privada”.
- “Utilización del programa de utilidad gencsr (opcional)” en la página 167 (opcional).
- “Registro de la CSR con la autoridad de certificación” en la página 169.
- “Instalación del certificado del servidor” en la página 169.
- “Actualización del archivo de configuración de Security Manager” en la página 169.
- “Prueba de la instalación del nuevo certificado” en la página 170.

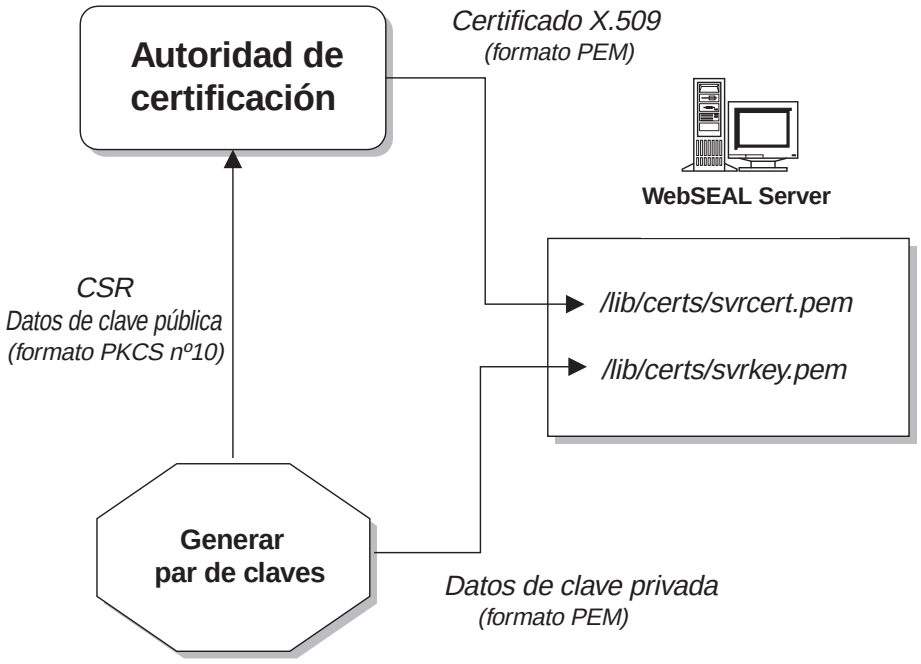
Generación de una clave pública y una clave privada

Para obtener un certificado local de una CA, primero debe generar un par de claves pública / privada para el servidor.

La porción correspondiente a la clave privada la conserva el usuario.

La porción correspondiente a la clave pública, que contiene información sobre la identidad del usuario, se conoce como petición de firma de certificado (Certificate Signing Request, CSR). La CSR es la información que deberá enviar a la CA cuando se registre para conseguir un certificado de servidor local. La CA utiliza esta información para crear el certificado X.509 del área del servidor que se utiliza para responder a clientes habilitados para SSL.

La clave privada y el certificado X.509 del área del servidor procedente de la CA deben almacenarse en ubicaciones designadas específicamente. El archivo de configuración secmgrd.conf de Policy Director define esas ubicaciones.



Para generar un par de claves pública y privada, utilice la herramienta de generación y las instrucciones que proporcione la autoridad de certificación. Policy Director facilita un programa de utilidad (**gencsr**) que puede utilizarse cuando no se dispone de ningún otro programa de utilidad. En el apartado "Utilización del programa de utilidad gencsr (opcional)" se explica cómo generar un par de claves con **gencsr**.

Utilización del programa de utilidad gencsr (opcional)

Policy Director incluye un programa de utilidad opcional, **gencsr**, que genera un par de claves pública y privada. El programa de utilidad forma parte de la instalación de Policy Director y se encuentra en el directorio /bin:

UNIX: *vía-instalación*/bin/gencsr

Windows: *vía-instalación*\bin\gencsr

Formato PKCS#10

El programa de utilidad **gencsr** genera el par de claves. Este programa de utilidad graba la información sobre la clave privada en un archivo en formato PEM. Este programa de utilidad almacena la clave pública en un archivo con el resto de la información de petición de firma de certificado. El programa de utilidad almacena la información de clave pública en formato PKCS#10.

Public-Key Cryptography Standards (PKCS) describe la sintaxis de las peticiones de certificación. Una petición de certificación está formada por un nombre distinguido, una clave pública y un conjunto de atributos opcional, firmados colectivamente por la organización al solicitar la certificación. Una petición de firma de certificado se envía a una autoridad de certificación. La CA genera entonces un certificado X.509 exclusivo de clave pública para el servidor.

Sintaxis del mandato del programa de utilidad gencsr

`gencsr [-csrfile archivo_csr] [-keyfile archivo_claves] [-keylen longitud_clave] [-version]`

Opciones	Descripción
-csrfile	Especifica la salida de clave pública (CSR) a un archivo (formato PKCS#10). El archivo especificado (*archivo_csr*) contiene la CSR en formato American National Standard Code for Information Interchange (ASCII). El valor por omisión es la salida estándar.
-keyfile	Indica la salida de la clave privada (en formato PEM) a un archivo. El valor por omisión es la salida estándar.
-keylen	Especifica la longitud de la clave (en bytes) del par de claves pública/privada. El valor por omisión es 512.
-version	Visualiza el número de versión del programa de utilidad y la información de copyright.
-help	Visualiza la sintaxis del mandato y las descripciones de las opciones.

Procedimientos del programa de utilidad gencsr

Para utilizar el programa de utilidad **gencsr** de Policy Director:

1. Inicie el programa de utilidad **gencsr** con los argumentos adecuados para indicar los nombres del archivo CSR, el archivo de la clave privada y, opcionalmente, una longitud de clave:

   UNIX: `$ gencsr -csrfile nombrearchivo -keyfile nombrearchivo -keylen 1024`

   Windows: `gencsr -csrfile nombrearchivo -keyfile nombrearchivo -keylen 1024`

   Puede utilizar cualquier nombre de archivo para las claves pública y privada; posteriormente ya les cambiará el nombre.

   Nota: La longitud de clave por omisión es 512 bytes.

2. El programa de utilidad solicita información personal, incluida la *frase de contraseña PEM*.

   Debe recordar esta frase de contraseña. Almacene posteriormente la frase de contraseña en el archivo de configuración secmgrd.conf. La frase de contraseña proporciona protección a la clave privada.

3. El programa de utilidad genera un archivo CSR y un archivo de clave privada. El apartado “Registro de la CSR con la autoridad de certificación” en la página 169 explica cómo enviar la CSR a la autoridad de certificación.

4. Haga una copia de seguridad del archivo de clave privada de ejemplo que se facilita con Policy Director:

   UNIX: `# cp svrkey.pem svrkey.pem.orig`

   Windows: `copy svrkey.pem svrkey.pem.orig`

5. Almacene el archivo de la clave privada que acaba de generar en este mismo directorio y llámelo svrkey.pem:

   UNIX: `# cp newkey.txt svrkey.pem`

Windows: `copy newkey.txt svrkey.pem`

Nota: Es necesario proteger esta clave privada. Debe haber una sola instancia de la clave privada, que es vital para comprobar la comunicación entre el cliente y el servidor.

Registro de la CSR con la autoridad de certificación

Para registrar la CSR con la autoridad de certificación:

1. Normalmente, la autoridad de certificación tiene un formulario de certificación en línea. Utilice un navegador Web para rellenar el formulario. Los procedimientos exactos son distintos según la CA.
2. El formulario de registro requiere que se proporcione la CSR generada en los apartados “Generación de una clave pública y una clave privada” en la página 166 o “Utilización del programa de utilidad gencsr (opcional)” en la página 167. Puede pegar el contenido del archivo de la CSR en el formulario o enviar el archivo por correo electrónico.
3. La CA envía el nuevo certificado público X.509 del área del servidor en formato PEM. Puede tardar varios días.

WebSEAL requiere que el certificado esté en formato PEM. La codificación PEM es una transformación de base64 que se aplica a un certificado binario. El formato PEM es un archivo ASCII en el que las líneas pueden tener como máximo 64 caracteres de longitud. El archivo ASCII empieza por:

```
-----BEGIN CERTIFICATE----
```

y termina por:

```
-----END CERTIFICATE----
```

Instalación del certificado del servidor

Para instalar el certificado del servidor:

1. Haga una copia de seguridad del archivo del certificado de ejemplo que se facilita con Policy Director:

   Para el formato PEM:

   UNIX: `# cp svrcert.pem svrcert.pem.orig`

   Windows: `copy svrcert.pem svrcert.pem.orig`
2. Almacene el nuevo archivo del certificado del servidor procedente de la CA en el mismo directorio y llámelo svrkey.pem (grábelo encima del valor antiguo):

   UNIX: `# cp newcert.txt svrcert.pem`

   Windows: `copy newcert.txt svrcert.pem`

Actualización del archivo de configuración de Security Manager

Compruebe y actualice si es necesario las siguientes entradas del archivo de configuración secmgrd.conf:

`certificate-file =`	El nombre de la vía de acceso al archivo que contiene el certificado en formato PEM recibido de la CA. Por omisión: lib/certs/svrcert.pem

key-file =	El nombre de la vía de acceso al archivo de la clave privada generada localmente. Por omisión: lib/certs/svrkey.pem
pass-key =	La frase de contraseña PEM utilizada para proteger la clave privada.

Cambie únicamente las entradas certificate-file y el key-file cuando utilice nombres de archivos distintos de los nombres de archivos por omisión listados.

Prueba de la instalación del nuevo certificado

Para probar la instalación del nuevo certificado:

1. Detenga y reinicie Policy Director para empezar a utilizar el nuevo certificado.

   UNIX:

   ```
   # /etc/init.d/iv stop
   # /etc/init.d/iv start
   # /etc/init.d/iv status
   ```

   Windows: Utilice el Panel de control Servicios.

2. Asegúrese de que Security Manager (secmgrd) se ha iniciado correctamente.

   Cuando secmgrd no se inicie correctamente, examine el siguiente archivo de anotaciones cronológicas para saber el motivo de la anomalía:

   UNIX: *vía-instalación*/secmgr/log/secmgrd.log

   Windows: *vía-instalación*\secmgr\log\secmgrd.log

   Si no encuentra ningún mensaje de error significativo, inicie secmgrd en modalidad de depuración. Consulte el apartado “Modalidad de depuración para dirigir mensajes a la salida estándar” en la página 150. También puede buscar la información más actual sobre corrección de problemas en el sitio Web de IBM SecureWay Policy Director:

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

3. Desde un navegador, conéctese al servidor que utilice HTTPS y asegúrese de que el navegador acepta el certificado del servidor.

   Por ejemplo, el navegador ya debe tener almacenado, por omisión, el ampliamente reconocido certificado root de VeriSign. Por lo tanto, no debería recibir ningún mensaje de aviso ni visualizar ningún recuadro de diálogo antes del indicador de inicio de sesión de Policy Director.

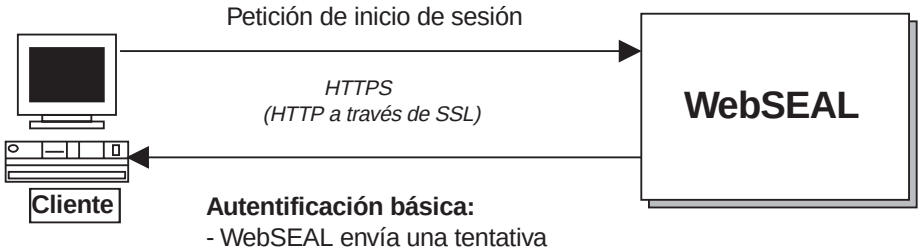
   Aparecerán mensajes de aviso si utiliza el certificado de ejemplo que se envía con Policy Director. Los mensajes de aviso se visualizarán porque el navegador no contiene ningún certificado root de IBM para verificar el certificado de ejemplo del servidor. Estos mensajes piden que se acepte o rechace el certificado del servidor. Cuando no hay ningún certificado root, el navegador no puede verificar la legitimidad del certificado del servidor. Por este motivo, el navegador deberá pasar al usuario la responsabilidad de aceptar o denegar el certificado.

   Ahora tiene en su sitio un certificado de servidor local validado por una autoridad de certificación fiable. Con el certificado del servidor validado almacenado en el lugar correcto, los clientes habilitados para SSL podrán autentificar de forma segura y satisfactoria el Policy Director WebSEAL Server.

Métodos de autentificación de nombre de usuario y de contraseña

Los mecanismos de autentificación Kerberos y LDAP Secret Key requieren información sobre la identidad del cliente en forma de un nombre de usuario y una contraseña. WebSEAL tiene soporte para dos métodos que proporcionen nombres de usuario y contraseñas para la autentificación:

- "Método de autentificación básica".
- "Método de inicio de sesión basado en formularios de Policy Director" en la página 172.



Autentificación básica:
- WebSEAL envía una tentativa
- El navegador produce una solicitud de inicio de sesión

Inicio de sesión basado en formularios:
- WebSEAL envía un formulario de inicio de sesión

Método de autentificación básica

WebSEAL tiene soporte para el protocolo de SSL, utilizado por Netscape® Communicator/Navigator y Microsoft Internet Explorer™ (IE) para obtener información sobre usuarios como, por ejemplo, nombres de usuario y contraseñas. Por convenio, los URL que indican la utilización de una conexión SSL segura empiezan por **https:** en vez de **http:**.

Para que el inicio de sesión sea correcto, Policy Director requiere que los clientes utilicen la identidad de Policy Director registrada en el registro de seguridad. La *autentificación básica* es un método estándar para proporcionar un nombre de usuario y una contraseña al mecanismo de autentificación.

En el primer paso, el servidor se autentifica ante el cliente utilizando el certificado del área del servidor. Si el cliente acepta el certificado, el servidor emitirá una tentativa para el cliente. El navegador producirá un indicador de inicio de sesión solicitando un nombre de usuario y una contraseña.

Nota: El navegador coloca en la antememoria esta información de iniciar sesión. La autentificación básica estándar requiere la información de nombre de usuario y de contraseña para cada petición subsiguiente. La información de autentificación colocada en la antememoria se envía al usuario de forma transparente.

Los puntos más importantes de la autentificación básica son los siguientes:

- Policy Director utiliza SSL como canal de comunicación seguro.
- Policy Director transmite los nombres de usuarios y las contraseñas a través del canal SSL seguro.

Puede que se visualice un indicador de inicio de sesión, a consecuencia de una tentativa de autentificación básica, parecido a éste:

```
Enter username for Policy Director [/.../www.ibm.com] at www.ibm.com

User Name:
Password:
```

Donde deberá entrar la información necesaria en los campos **User Name** (Nombre de usuario) y **Password** (Contraseña).

Modelo de autentificación básica

El proceso de los modelos de autentificación básica es el siguiente:

1. Un navegador cliente se pone en contacto con el servidor utilizando SSL.
2. El servidor devuelve el certificado de clave pública firmado que ha obtenido de la CA.
3. El navegador cliente lleva a cabo una de estas operaciones:
   - Busca un certificado root de CA en su base de datos y acepta el certificado del servidor.
   - No tiene ningún certificado root de CA en la base de datos y envía un aviso al usuario. El usuario tendrá entonces la responsabilidad de aceptar o rechazar el certificado.
4. Cuando se acepta, el servidor emite una tentativa para el navegador.
5. El navegador responde produciendo un indicador de inicio de sesión solicitando un nombre de usuario y una contraseña.
6. Cuando el usuario ha escrito la información de nombre de usuario y contraseña, el navegador envía la información al servidor Policy Director.
7. Policy Director produce una credencial cuando la información de nombre de usuario y contraseña coincide con la información existente en el registro de usuarios de Policy Director. Policy Director utiliza la credencial para tomar decisiones de autorización. WebSEAL coloca en la antememoria esa credencial para el tiempo que dure la sesión SSL.
8. El navegador coloca en la antememoria la información del nombre de usuario y la contraseña.

   La autentificación estándar básica requiere ese nombre de usuario y contraseña para cada inicio de sesión o petición subsiguientes del navegador. Este requisito se satisface de forma transparente utilizando la información de autentificación guardada en la antememoria.

   Nota: Como en la autentificación básica el navegador coloca en la antememoria la información de nombre de usuario y contraseña, el mandato **pkmslogout** no funciona correctamente. Para finalizar la sesión completamente, cierre la sesión del navegador. Utilice el inicio de sesión basado en formularios cuando requiera la función **pkmslogout**.

Tareas administrativas necesarias

Para preparar WebSEAL Server para el acceso a SSL en modalidad de autentificación básica, el administrador debe realizar las siguientes tareas:

- Instalar el certificado X.509 del área del servidor en el WebSEAL Server.
- Crear una cuenta de Policy Director para cada usuario que vaya a participar del dominio seguro.

Método de inicio de sesión basado en formularios de Policy Director

Policy Director tiene una alternativa al mecanismo de autentificación estándar básica: el *inicio de sesión basado en formularios* de Policy Director. Este método

produce un formulario HTML de inicio de sesión de Policy Director en vez del indicador de inicio de sesión estándar que se produce tras una tentativa de autentificación básica.

Cuando se utiliza el inicio de sesión basado en formularios, el navegador no coloca en la antememoria la información de nombre de usuario y contraseña como lo hace en la autentificación básica. Esto permite utilizar satisfactoriamente el mandato especial de fin de sesión SSL **pkmslogout**. Como Policy Director requiere la información de credenciales una sola vez (y la coloca en la antememoria), no será necesario repetir las peticiones de inicio de sesión en cada petición del navegador.

Para realizar un inicio de sesión basado en formularios, utilice el parámetro **https-forms-auth** de la sección [wand] del archivo de configuración iv.conf. Este parámetro puede tener el valor yes (sí) o no. El valor por omisión es no.

```
[wand]
https-forms-auth = no
```

Policy Director incluye siete formularios HTML de ejemplo. Puede personalizar estos formularios HTML para que contengan mensajes específicos de la ubicación o para que realicen acciones específicas de la ubicación.

La sección [wand] del archivo de configuración iv.conf define las ubicaciones de los archivos donde se encuentran esos formularios en SSL HTML Page Locations.

La ubicación por omisión del directorio es:

UNIX: *vía-instalación*/www/lib/html/

Windows: *vía-instalación*\www\lib\html\

Formulario	Descripción
login.html	Petición de nombre de usuario y contraseña
login_rep.html	Mensaje de error de inicio de sesión
logout.html	Mensaje de fin de sesión correcto de la sesión SSL
passwd.html	Formulario de cambio de contraseña
passwd_exp.html	Mensaje de contraseña caducada
passwd_rep.html	Mensaje de error de cambio de contraseña
help.html	Consulta de mandatos

Estas páginas también contienen dos macros que pueden utilizarse. Puede colocarlas en los archivos de plantillas. La rutina las sustituirá dinámicamente por los valores adecuados.

Macro	Descripción
%USERNAME%	El nombre del usuario que ha iniciado la sesión.
%ERROR%	El mensaje de error codificado en origen devuelto por Policy Director.

Modelo de autentificación basado en formularios

El modelo de autentificación basado en formularios sigue este proceso:

1. Un navegador cliente se pone en contacto con el servidor utilizando SSL.
2. El servidor devuelve el certificado de clave pública firmado que ha obtenido de la CA.

3. El navegador cliente lleva a cabo una de estas operaciones:
   - Busca un certificado de CA asociado en su base de datos y acepta el certificado del servidor.
   - No tiene ningún certificado de CA asociado en la base de datos y envía un aviso al usuario. El usuario tendrá entonces la responsabilidad de aceptar o rechazar el certificado.
4. Si el cliente lo acepta, WebSEAL solicita al cliente un nombre de usuario y una contraseña utilizando un formulario HTML de Policy Director personalizado.

   Policy Director utiliza el formulario para devolver a WebSEAL la información de nombre de usuario y contraseña.
5. Policy Director produce una credencial cuando la información de nombre de usuario y contraseña coincide con la información existente en el registro de usuarios de Policy Director. Policy Director utiliza la credencial para tomar decisiones de autorización. WebSEAL coloca en la antememoria esa credencial para el tiempo que dure la sesión SSL.

   A diferencia de la autentificación básica, el navegador *no* coloca en la antememoria la información de nombre de usuario y contraseña. El mandato **pkmslogout** funciona ahora correctamente.

Tareas administrativas necesarias

Para preparar WebSEAL Server para el acceso a SSL en modalidad de inicio de sesión basado en formularios, el administrador debe realizar las siguientes tareas:

1. Instalar el certificado X.509 de CA del área del servidor en el WebSEAL Server.
2. Crear una cuenta de Policy Director para cada usuario que vaya a participar del dominio seguro.
3. Personalizar los formularios de Policy Director y definir su ubicación en el archivo de configuración iv.conf.

Mandatos para métodos de nombre de usuario y contraseña

Policy Director proporciona los siguientes mandatos para dar soporte a la autentificación de clientes con SSL habilitado utilizando el método de nombre de usuario y contraseña:

- pkmslogout
- pkmspasswd

pkmslogout

Utilice el mandato pkmslogout para finalizar la sesión SSL actual. Este mandato es adecuado para el método de inicio de sesión basado en formularios.

```
https: //Web URL vía-instalación/pkmslogout
```

Por ejemplo:

```
https: /www.ibm.com/pkmslogout
```

El archivo que se visualiza en respuesta al fin de sesión se define en el archivo de configuración iv.conf.

```
# SSL HTML page
locations
pkms-logout-page = lib/html/logout.html
```

Puede cambiar el archivo logout.html para que se adapte a sus necesidades.

El programa de utilidad **pkmslogout** también tiene soporte para varias páginas de respuestas de fin de sesión por si la arquitectura de la red requiere distintas pantallas de salida para usuarios que finalicen la sesión desde sistemas principales claramente diferentes.

La siguiente expresión especifica un archivo de respuestas determinado:

`https://pkmslogout?filename=`*`arch_fin_sesión_personalizado`*

Donde *arch_fin_sesión_personalizado* es el nombre del archivo de respuesta de fin de sesión. El archivo debe residir en el mismo directorio /lib/html/ definido para el archivo logout.html por omisión.

pkmspasswd

Ejecute este mandato para cambiar la contraseña.

`https://`*`Web URL vía-instalación`*`/pkmspasswd`

Por ejemplo:

`https://www.ibm.com/pkmspasswd`

Método de autentificación de certificado X.509

WebSEAL tiene soporte para la autentificación utilizando un certificado X.509 del área del cliente a través de SSL. El certificado X.509, en vez del nombre de usuario y la contraseña, proporciona la información de identidad del cliente.

Tareas de configuración para el soporte de certificados X.509 del área del cliente

Realice las siguientes tareas para configurar WebSEAL de forma que acepte certificados digitales X.509 del área del cliente:

Tareas del cliente

Para realizar tareas de cliente:

1. Obtenga de una CA un certificado digital X.509 del área del cliente (clave pública firmada).
2. Instale el certificado en el sistema cliente.

Tareas de WebSEAL Server

Para efectuar tareas de WebSEAL Server:

1. Obtenga el certificado root de CA de la misma autoridad de certificación.

   El certificado puede tener formato PEM o PKCS#12.
2. Copie el certificado root de CA en la ubicación adecuada del sistema e indique dicha ubicación en el archivo de configuración secmgrd.conf:

   Formato PEM:

   Añada los certificados root al siguiente archivo:

   UNIX: `ca-cert-file = lib/certs/cacert.pem`

   Windows: `ca-cert-file = lib\certs\cacert.pem`

   Formato PKCS#12:

   Añada cada certificado root como un archivo separado en el siguiente directorio:

   UNIX: `ca-cert-p12-dir = lib/certs/ca_p12`

   Windows: `ca-cert-p12-dir = lib\certs\ca_p12`

Nota: Estos certificados con formato PEM y formato PKCS#12 son certificados de las autoridades de certificación que Policy Director considera fiables.

3. Se puede indicar cómo debe gestionar WebSEAL los certificados X.509 del área del cliente definiendo el parámetro **verify-clients** (verificar clientes). Entre uno de los siguientes valores permitidos para verify-clients en la sección [wand] del archivo de configuración iv.conf: never, optional o required.

   En el apartado “Configuración de la gestión de certificados” en la página 164 encontrará las descripciones de estos valores.

4. Configure WebSEAL para utilizar el servidor CAS editando el archivo iv.conf y modificando el parámetro **cert-cdas** de la sección [authentication-mechanisms] para que se adapte a las necesidades de la plataforma correspondiente:

   ```
   [authentication-mechanisms]
   cert-cdas = &entry=/.:/subsys/intraverse/cdas/servers/nombre
   sistema principal
   ```

   Entre las opciones posibles para el *módulo cas* se incluyen cdasauthn.dll para Windows NT, libcdasauthn.a para AIX y libcdasauthn.so para Solaris.

   En el apartado “Configuración básica de Policy Director CAS” en la página 178 encontrará información detallada sobre el parámetro **cert-cdas**.

5. Defina la identidad del servidor utilizando los parámetros **certificate-file** y **key-file** del archivo de configuración secmgrd.conf. Tenga en cuenta que la clave privada del servidor está en formato PEM. Los parámetros son distintos, dependiendo de la plataforma para la que se utilizan:

   Parámetro certificate-file en formato PEM:

   UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.pem`

   Windows: `certificate-file = C:\Archivos de programa\ibm\Policy Director\lib\certs\svrcert.pem`

   Parámetro key-file en formato PEM:

   UNIX: `key-file = /opt/intraverse/lib/certs/srvkey.pem`

   Windows: `key-file = C:\Archivos de programa\ibm\Policy Director\lib\certs\srvkey.pem`

   En el apartado “Almacenamiento de certificados” en la página 163 encontrará información sobre los parámetros de almacenamiento de certificados de secmgrd.conf.

6. Defina la identidad del servidor utilizando el parámetro certificate-file del archivo de configuración secmgrd.conf. Tenga en cuenta que el certificado del servidor está en formato PKCS#12:

   Parámetro certificate-file en formato PKCS#12:

   Para UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.p12`

   Para Windows: `certificate-file = C:\Archivos de programa\ibm\Policy Director\lib\certs\svrcert.p12`

7. Utilice Policy Director Credentials Acquisition Service (CAS) para la adquisición y correlación de credenciales.

   También puede escribir e instalar su propio programa de adquisición y correlación de credenciales en el sistema servidor. En el manual *Policy Director Programmer's Guide and Reference* y en el apartado “Configuración de Policy Director Credentials Acquisition Service” en la página 177 encontrará más información.

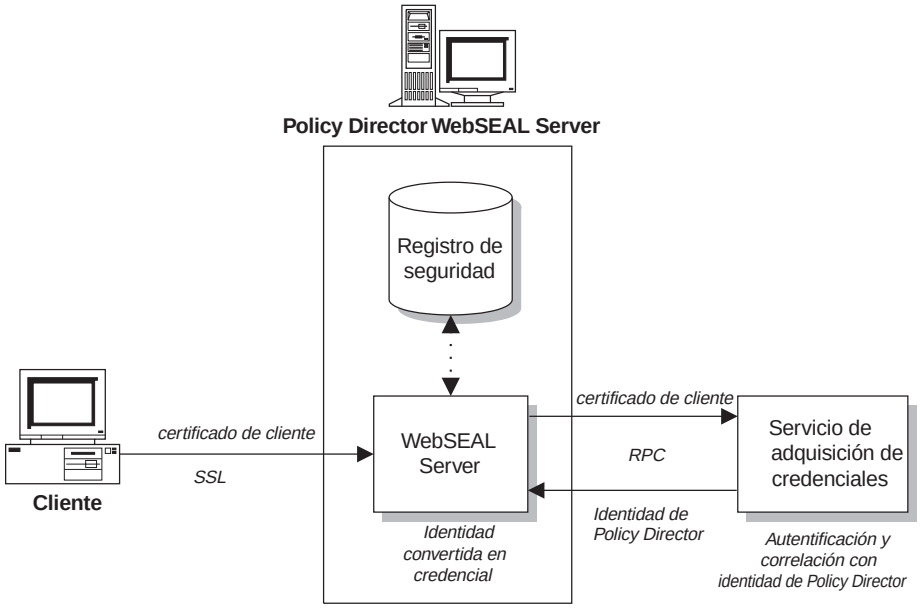
Configuración de Policy Director Credentials Acquisition Service

El servicio Policy Director Credentials Acquisition Service (CAS) es un componente personalizable que puede utilizarse para ampliar los mecanismos de autentificación estándar soportados por WebSEAL. El servicio Policy Director Credentials Acquisition Service por omisión utiliza el archivo cdas_server(.exe). Consulte el apartado “Configuración de WebSEAL para utilizar Policy Director CAS”.

También puede escribir e instalar su propio programa de adquisición y correlación de credenciales en el sistema servidor. En el manual *Policy Director Programmer’s Guide and Reference* encontrará información para escribir e instalar un servicio de adquisición de credenciales.

Presentación de Policy Director CAS

Policy Director Credentials Acquisition Service (CAS) permite la autentificación y correlación de información sobre la identidad de un usuario (como, por ejemplo, el certificado X.509) con la identidad de un usuario de Policy Director. Security Manager (utilizando su registro por omisión) devuelve las credenciales de la identidad de dicho usuario.



En los apartados “CAS proporcionado por Policy Director” en la página 32 y “Configuración de WebSEAL para utilizar Policy Director CAS” encontrará información sobre Policy Director CAS.

Configuración de WebSEAL para utilizar Policy Director CAS

Puede configurar todos los mecanismos de autentificación soportados por WebSEAL en la sección `authentication-mechanisms` del archivo de configuración iv.conf. Todos los mecanismos de autentificación soportados por WebSEAL pueden ser tanto autentificadores locales (proceso interno) como autentificadores remotos personalizados activados por servidores de CAS.

Módulos de conexiones (plugin) locales

En el archivo de configuración, cada autentificador se asocia con un módulo de conexiones (plugin) local. En las plataformas UNIX, estos módulos son bibliotecas compartidas. En Windows NT, estos módulos son Dynamic Link Libraries (DLL). Estos módulos proporcionados como una parte estándar de la distribución de Policy Director no pueden personalizarse.

Policy Director proporciona un módulo de conexiones estándar. Utilice el módulo de conexiones (plugin) para intercambiar información con cualquier servidor de CAS de terceros:

Plataforma	Nombre de módulo de CAS
Solaris	libcdasauthn.so
AIX	libcdasauthn.a
Windows NT	cdasauthn.dll

Configuración básica de Policy Director CAS

Puede configurar un servicio Policy Director Credentials Acquisition Service que se refiera a la información de certificados X.509, que lleva a cabo la autentificación del área del cliente de la interfaz CAS de WebSEAL. La configuración de Policy Director CAS requiere un argumento adicional que representa la ubicación en el espacio de nombres de los CDS de DCE donde está almacenada la información del enlace lógico del servidor CAS.

Para configurar WebSEAL de forma que utilice un servidor CAS, edite el archivo iv.conf y modifique el parámetro cert-cdas de la sección [authentication-mechanisms] para que se adapte a las necesidades de la plataforma correspondiente.

Por ejemplo, la siguiente secuencia de configuración (para Windows NT) identifica un solo servidor CAS que tiene soporte para la autentificación básica basada en certificados X.509:

```
[authentication-mechanisms]
cert-cdas = cdasauthn.dll&entry=/.:/subsys/intraverse/cdas/servers/nombre sistema principal
```

Donde `cdasauthn.dll` representa el módulo CAS de la plataforma correspondiente, *nombre sistema principal* es el nombre simple del sistema principal y `&entry=/.:/subsys/intraverse/cdas/servers/`*nombre sistema principal* representa la ubicación en el espacio de nombres de los CDS de DCE donde se almacena la información del enlace lógico del servidor CAS.

Sintaxis de entrada de configuración

Una entrada de configuración de autentificación tiene el siguiente formato:

```
authn-mechanism = module[&arg1[
arg2]...[ argN]]
```

Múltiples servidores CAS de Policy Director

Un solo Policy Director Credentials Acquisition Service puede soportar más de un mecanismo de autentificación. En ese caso, cada mecanismo tendrá una información de configuración duplicada.

Correlación de nombres distinguidos

Policy Director CAS correlaciona *certificados digitales de clientes* procedentes del navegador habilitado para SSL con una identidad de usuario de Policy Director. Cuando el usuario intenta acceder a una página Web protegida, 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. Policy Director CAS intenta correlacionar el certificado que ha recibido con una identidad de usuario que Policy Director pueda entender.

Dentro del archivo de configuración cdas.conf de Policy Director CAS, el administrador de Policy Director puede crear una tabla que se utilice para asociar un nombre distinguido (DN) de certificado con el DN de un usuario de Policy Director. Cuando WebSEAL llama a Policy Director CAS con un certificado, primero extrae el DN del certificado y comprueba si hay alguna coincidencia en la tabla. Si encuentra una coincidencia, Policy Director Credentials Acquisition Service devuelve a WebSEAL el DN del usuario asociado de Policy Director formateado correctamente. Este método se denomina *correlación de DN*.

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 (LDAP). WebSEAL Server usa el DN devuelto para recuperar las credenciales del usuario.

El archivo de configuración cdas.conf para la correlación de nombres distinguidos puede encontrarse en:

UNIX: `/opt/intraverse/cdas_server/lib/cdas.conf`

Windows: `C:\Archivos de programa\IBM\Policy Director\cdas_server\lib\cdas.conf`

El archivo de configuración cdas.conf contiene la siguiente información:

```
# Correlación de DN

# Si el DN del certificado se encuentra en la tabla siguiente use el DN
# correspondiente de LDAP. De lo contrario, utilice el DN del certificado
# tal como está.
# Cada entrada debe estar en una sola línea con el siguiente formato:
# [DN del certificado]DN de LDAP con el que va a hacerse la correlación.
# Por ejemplo:
# [/C=US/O=IBM/CN=Usario Policy Director] cn=Usuario Policy Director,o=IBM,c=US
# [/C=US/O=IBM/CN=Usuario1] cn=Usuario IBM Policy Director,o=IBM,c=US
```

El nombre distinguido (DN) del certificado se encuentra siempre a la izquierda de la tabla y está siempre entre corchetes: `[/C=US/O=IBM/CN=Usuario de Policy Director]`. El DN del usuario de Policy Director (igual que el DN del registro LDAP) está siempre a la derecha de la tabla. `cn=Usuario de Policy Director,o=IBM,c=US`. El DN de usuario de Policy Director sigue siempre al corchete derecho del DN del certificado y requiere un espacio en blanco a continuación. Para que el funcionamiento sea correcto, los dos lados de entradas de la tabla de correlación deben cumplimentarse por orden.

Los navegadores habilitados para SSL, como Netscape® Communicator / Netscape Navigator® y Microsoft Internet Explorer™, permiten ver información de DN de los certificados. La información de DN para estos navegadores puede visualizarse de varias formas, pero la información de certificados para ambos navegadores debe contener todos los elementos de los nombres distinguidos.

Capítulo 14. WebSEAL: Tareas generales de administración

Este capítulo contiene información que describe las tareas generales de administración y de configuración que pueden realizarse para personalizar WebSEAL en la red.

Este capítulo incluye los siguientes temas:

Habilitación e inhabilitación de la seguridad de WebSEAL

Utilice el programa de utilidad **ivadmin** para habilitar e inhabilitar WebSEAL.

Para habilitar WebSEAL en un servidor específico de Policy Director:

```
ivadmin> server enable /WebSEAL/
```

El nombre del sistema principal es el nombre del servidor excluyendo el nombre de dominio.

Cuando el servicio ya se ha habilitado o cuando la especificación de servicio no es válida, Policy Director devuelve errores.

Por omisión, Policy Director habilita WebSEAL.

Para inhabilitar WebSEAL en un servidor específico de Policy Director, utilice el mandato **ivadmin server disable**:

```
ivadmin> server disable /WebSEAL/
```

Para comprobar el estado de WebSEAL Server, utilice el mandato **ivadmin server status**:

```
ivadmin> server status nombre-sistema-principal
```

El informe de estado visualiza la siguiente información:

- Si el servidor WebSEAL está inhabilitado o inhabilitado.
- Si se puede llegar a WebSEAL Server utilizando PING.
- El estado de la base de datos de configuración de WebSEAL.

Gestión del espacio de la Web

Esta sección describe las tareas necesarias para gestionar el espacio de nombres de WebSEAL:

- “Especificación de tipos de extensión de archivos para programas CGI” en la página 183 .

Especificación de las ubicaciones del árbol de documentos Web

La ubicación del árbol de documentos Web es la vía de acceso absoluta al root del árbol de documentos que el servidor deja disponible. La ubicación por omisión se establece inicialmente durante la instalación de Security Manager:

UNIX: *vía-instalación*/www/docs

Windows: *vía-instalación*\www\docs

Esta ubicación puede cambiarse utilizando el script de instalación. Tras la instalación, deberá utilizar el programa de utilidad **junctioncp** para cambiar esta ubicación. En el apartado “Utilización de junctioncp para gestionar conexiones Smart Junction” en la página 197 encontrará la información completa sobre el mandato.

El siguiente ejemplo para UNIX ilustra la forma de utilizar el programa de utilidad **junctioncp** para cambiar la ubicación:

1. Ejecute **junctioncp**:

```
# junctioncp -e hostA
Intentando efectuar el enlace con hostA en
/.:/subsys/intraverse/secmgr/server/hostA
junctioncp>
```

2. Utilice el mandato **list** para visualizar todos los puntos de conexión Smart Junction actuales:

```
junctioncp> list
/
```

3. Utilice el mandato **show** para visualizar detalles de la conexión (junction):

```
junctioncp> show /

Punto de conexión Smart Junction: /
Tipo: Root local
Directorio: /opt/intraverse/www/docs
```

4. Cree una nueva conexión (junction) local para sustituir el punto de conexión actual:

```
junctioncp> create -t local -d /tmp/docs /
AVISO: Ya existe una conexión (junction)
¿Desea sustituirla? [no]? sí
Se ha creado una conexión (junction) en /
```

5. Liste el nuevo punto de conexión Smart Junction:

```
junctioncp> list
/
```

6. Visualice los detalles de la conexión (junction):

```
junctioncp> show /

Punto de conexión Smart Junction: /
Tipo: Root local
Directorio: /tmp/docs
```

Configuración de la creación de índices de directorios

Puede especificar el nombre del archivo por omisión que devuelve el servidor. Se especifica cuando se proporciona un nombre de directorio como URL. Policy

Director devuelve este archivo por omisión al cliente cuando existe. Si no existe, Policy Director genera dinámicamente y devuelve un índice de directorio al cliente.

Nota: Policy Director no almacena en disco el índice generado. Policy Director recupera el índice de la antememoria del ″wand″ o del índice de directorios (″dirindex″) del servidor, o regenera el índice cada vez que se accede al directorio.

Los parámetros para configurar la creación de índices de directorios se encuentran en la sección [wand-indexing] del archivo de configuración iv.conf.

El valor del archivo por omisión es:

```
[wand-indexing]
dirindex = index.html
```

Si su empresa utiliza un convenio distinto, podrá cambiar este nombre de archivo:

```
[wand-indexing]
dirindex = default.html
```

Cada parámetro utilizado para crear índices de directorios tiene un icono por omisión (archivo .gif) que se visualiza para cada tipo de documento y para cada tipo de MIME encontrado:

```
[wand-indexing]
image/*= /icons/image2.gif
video/* = /icons/movie.gif
audio/* = /icons/sound2.gif
text/html = /icons/html.gif
text/* = /icons/text.gif
application/* = /icons/binary.gif
```

Puede especificar otros iconos para cada parámetro. También puede ubicar iconos de forma remota y utilizar los URL como valores de parámetros. Por ejemplo:

```
application/* = http://www.acme.com/icons/binary.gif
```

Especificación de tipos de extensión de archivos para programas CGI

Los parámetros contenidos en la sección [wand-cgi-types] del archivo de configuración iv.conf permiten especificar tipos de extensión de archivos de Windows. Policy Director reconoce los tipos de extensión de archivos de Windows que pueden iniciarse como programas CGI.

El sistema operativo UNIX no tiene ningún requisito sobre las extensiones de nombres de archivos. No obstante, deben definirse los tipos de extensión de nombres de archivos para Windows NT. La sección [wand-cgi-types] indica todos los tipos de extensión válidos y correlaciona cada extensión (cuando es necesario) con un programa CGI adecuado.

Por omisión, Policy Director inicia únicamente los archivos cuyas extensiones coincidan con las listadas en la sección como programas CGI. Por omisión, Policy Director ejecuta los archivos que tienen las extensiones .exe como programas y dichos archivos no requieren correlación. Debe suministrar los programas intérprete adecuados para las extensiones que indiquen archivos de scripts interpretados. Los tipos de extensión son, por ejemplo, scripts de shell (.sh y .ksh), scripts Perl (.pl), y scripts Tcl (.tcl).

El siguiente ejemplo ilustra una configuración típico de la sección [wand-cgi-types]:

```
#
# Extensión de archivo CGI para correlaciones de mandatos (sólo Windows NT)
#
# Para servidores WIN32 se nombran extensiones de archivos CGI y el programa
# utilizado para ejecutarlos. Si una CGI tiene una extensión que no se encuentre
# en esta lista, no se ejecutará.
#
[wand-cgi-types]
.exe =
.bat =
.cmd =
.pl = perl
.sh = sh
.tcl = tclsh76
```

Nota: La utilización de archivos .bat implica graves problemas. No utilice archivos .bat.

Configuración de hebras de trabajo HTTP y HTTPS

El número de hebras de trabajo configuradas especifica el número de peticiones simultáneas entrantes que un servidor puede atender. Cuando todas las hebras de trabajo están ocupadas, Policy Director coloca en el almacenamiento intermedio las otras conexiones que llegan hasta que una hebra de trabajo queda disponible.

Puede definir el número de hebras de forma que sea suficiente para atender a las peticiones de conexión entrantes. Configure cuidadosamente el número de hebras de trabajo ya que éste puede incidir en el rendimiento.

Este parámetro de configuración no impone un límite superior en el número de conexiones simultáneas. Este parámetro especifica simplemente el número de hebras disponibles para atender una cola de trabajos potencialmente ilimitada.

La selección del número óptimo de hebras de trabajo depende de que se asimile la cantidad y el tipo de tráfico de la red.

En general, al aumentar el número de hebras, disminuye el tiempo medio que se tarda en finalizar las peticiones. Sin embargo, al aumentar el número de hebras afecta a otros factores que podrían tener un efecto adverso en el rendimiento del servidor.

Definición del valor de la agrupación de hebras de trabajo para WebSEAL

WebSEAL mantiene una sola lista genérica de hebras de trabajo y mantiene también una agrupación de hebras de trabajo para gestionar las peticiones de clientes que utilicen TCP, SSL o la tunelización (″tunnel″) de GSS. Este mecanismo mejorado permite a WebSEAL utilizar menos recursos del sistema y manejar una carga significativamente mayor.

El tamaño de la agrupación de hebras de trabajo se controla definiendo el parámetro worker-threads en la sección [wand] del archivo de configuración iv.conf.

```
worker-threads = 50
```

Configuración de WebSEAL para peticiones HTTP

Normalmente, WebSEAL maneja muchas peticiones HTTP de usuarios no autentificados. Por ejemplo, es conveniente permitir a los usuarios desconocidos (y, por lo tanto, no autentificados) acceso de sólo lectura a determinados materiales de un sitio Web.

La sección [wand] del archivo de configuración iv.conf contiene parámetros para la gestión de peticiones HTTP a través de TCP.

Habilitación e inhabilitación de la escucha de HTTP

Por omisión, Policy Director habilita (permite) la escucha de peticiones HTTP a través de TCP:

```
allow-tcp-http = yes
```

Si se da a este parámetro el valor no, se inhabilita la escucha de HTTP.

Definición del valor de puerta

La puerta por omisión para la escucha de HTTP a través de TCP es 80:

```
http-tcp-port = 80
```

Para cambiar este valor por la puerta 8080, indique:

```
http-tcp-port = 8080
```

Configuración de WebSEAL para peticiones HTTPS

La sección [wand] del archivo de configuración iv.conf contiene parámetros para el manejo de peticiones HTTPS a través de SSL.

Habilitación e inhabilitación de la escucha de HTTPS

Por omisión, Policy Director habilita (permite) la escucha de peticiones HTTPS a través de SSL:

```
allow-ssl-http = yes
```

Si se da a este parámetro el valor no, se inhabilita la escucha de HTTPS.

Definición del valor de puerta

La puerta por omisión para la escucha de HTTPS a través de SSL es la 443:

```
ssl-port = 443
```

Para cambiar este valor por la puerta 4343, indique:

```
ssl-port =
4343
```

Especificación de parámetros de tiempo de espera

Pueden definirse, entre otros, los siguientes parámetros de tiempo de espera de Policy Director:

- Los parámetros de tiempo de espera para comunicaciones HTTP
- Parámetros adicionales de tiempo de espera de WebSEAL Server en la sección [wand] del archivo de configuración iv.conf

Parámetros de tiempo de espera para comunicaciones HTTP

WebSEAL tiene soporte para los siguientes parámetros de tiempo de espera para comunicaciones HTTPS:

ssl-init-connect-timeout (sólo HTTPS)

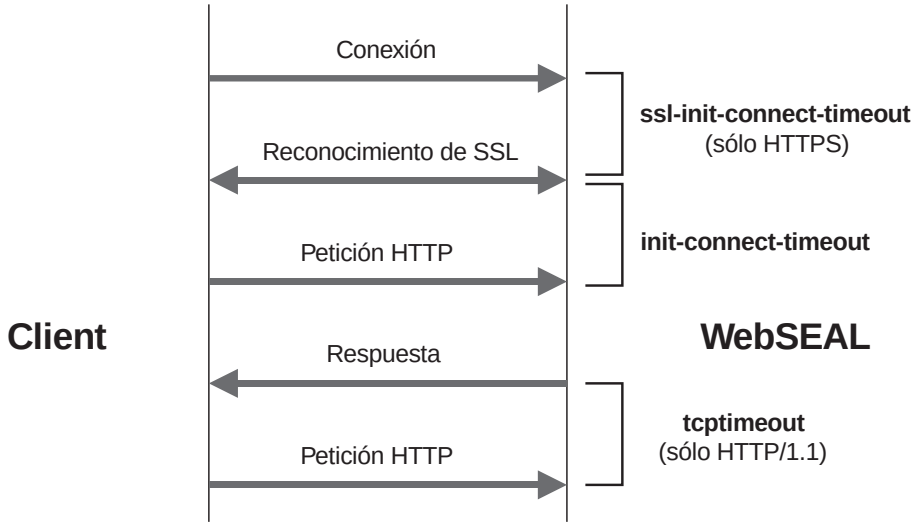
Cuando WebSEAL acepta una conexión SSL procedente de un navegador, debe producirse un *reconocimiento* del protocolo SSL. Un reconocimiento es el proceso en el que se intercambian señales para establecer las comunicaciones entre dos módems. Este parámetro controla el tiempo que Security Manager espera a que un navegador SSL inicie un reconocimiento de SSL. Esta incialización se produce al principio de una conexión SSL, antes de concluir la conexión.

init-connect-timeout

Después de haberse producido el reconocimiento de SSL, este parámetro indica cuándo tiempo debe esperar WebSEAL una petición inicial HTTP. La conexión puede ser HTTP, HTTPS o NetSEAT (HTTP y GSS).

tcptimeout

Este parámetro es específico de conexiones HTTP/1.1 (no de HTTP/1.0). Después de la primera petición HTTP/1.1 y de la primera respuesta del servidor, este parámetro controla el número máximo de segundos que el servidor mantiene abierta una conexión HTTP/1.1 permanente. La conexión concluye cuando se alcanza el número máximo de segundos.



Parámetro	Archivo de configuración	Valor por omisión (segundos)
ssl-init-connect-timeout	sección [ssl] de secmgrd.conf	120
init-connect-timeout	sección [wand] de iv.conf	120
tcptimeout	sección [wand] de iv.conf	5

Parámetros adicionales de tiempo de espera de WebSEAL Server

Los siguientes parámetros de tiempo de espera se definen en la sección [wand] del archivo de configuración iv.conf:

Parámetro	Descripción	Valor por omisión (segundos)

tcp-junction-timeout	El tiempo de espera para el envío y lectura desde un servidor principal a través de una conexión (junction) TCP.	120
ssl-junction-timeout	El tiempo de espera para el envío y lectura desde un servidor principal a través de una conexión (junction) SSL.	120
cgi-timeout	El tiempo de espera para el envío y lectura desde un proceso CGI local.	120
junction-ping-time	WebSEAL realiza un sondeo (PING) periódico de cada servidor conectado para determinar si está funcionando. WebSEAL sólo intenta esta operación cada 300 segundos (o el valor que se haya definido).	300

Configuración de mensajes de error HTTP

A veces, WebSEAL Server intenta atender una petición y la operación no se ejecuta correctamente. Este error puede deberse a muchas causas. Por ejemplo:

- Un archivo no existe.
- Los valores de permisos prohíben el acceso.
- Los permisos de un archivo UNIX no son correctos o pasa algo parecido que impide el inicio de los programas CGI.

Cuando se produce un error al intentar atender una petición, el servidor devuelve un mensaje de error al navegador como, por ejemplo `403 Prohibido`, en una página de error HTML. Hay varios mensajes de error disponibles. Un archivo HTML distinto almacena cada mensaje.

Los archivos se encuentran en el siguiente directorio:

UNIX:

vía-instalación`/www/lib/errors/`*dir-locales*

Windows:

vía-instalación`\www\lib\errors\`*dir-locales*

El directorio `errors` contiene varios subdirectorios de soportes nacionales (locales). Los subdirectorios contienen versiones locales de los archivos de mensajes de error.

Los mensajes de este directorio están en formato HTML para que puedan visualizarse correctamente en un navegador. Estas páginas HTML pueden editarse para personalizar su contenido. Los nombres de los archivos son los valores hexadecimales de los códigos de error interno que se devuelven cuando las operaciones no se ejecutan correctamente. No cambie los nombres de estos archivos.

La siguiente tabla contiene una lista de con los nombres de archivos y el contenido de algunos de los mensajes de error más comunes.

Nombre de archivo	Título	Descripción	Código de error HTTP

1354a2fa.html	El directorio no está vacío	La operación solicitada requiere la eliminación de un directorio que no está vacío. Esta operación no está permitida.	
1898d25a.html	No se ha podido conectar al usuario	El recurso solicitado necesita el WebSEAL Server para conectar al usuario con otro servidor Web. Sin embargo, se ha producido un problema mientras WebSEAL intentaba recuperar la información.	
1898d25b.html	El usuario no tiene información de conexión propia	WebSEAL no ha podido localizar al usuario de GSO para el recurso solicitado.	
1898d25c.html	No hay ningún destino de conexión propia para el usuario	WebSEAL no ha podido localizar al destino de GSO para el recurso solicitado.	
1898d25d.html	El usuario tiene varios destinos de conexión	Hay varios destinos de GSO definidos para el usuario solicitado. Los destinos de GSO se han configurado incorrectamente.	
1898d25e.html	Se necesita inicio de sesión	El recurso solicitado está protegido por un servidor Web principal y es necesario que WebSEAL conecte al usuario a este servidor Web. Para ello, primero el usuario debe iniciar la sesión con WebSEAL.	
1898d25f.html	No se ha podido conectar al usuario	El recurso solicitado necesita WebSEAL para conectar al usuario con otro servidor Web. Sin embargo, la información de conexión de la cuenta del usuario es incorrecta.	
1898d260.html	Tentativa de autentificación inesperada	WebSEAL ha recibido una tentativa de autentificación inesperado de un servidor Web principal conectado (junction).	
1898d421.html	Trasladado temporalmente	El recurso solicitado se ha trasladado temporalmente. Habitualmente, esto se produce cuando ha habido una redirección mal gestionada.	302
1898d424.html	Petición incorrecta	WebSEAL ha recibido una petición HTTP que no es válida.	400
1898d425.html	Se necesita inicio de sesión	El recurso que ha solicitado está asegurado por WebSEAL y para poder acceder a él primero debe iniciar la sesión.	
1898d427.html	Prohibido	El usuario no tiene permiso para acceder al recurso solicitado.	403
1898d428.html	No encontrado	No se ha podido localizar el recurso solicitado.	404
1898d432.html	Servicio no disponible	Un servicio que WebSEAL necesita para completar la petición no está disponible en ese momento.	503

1898d437.html	Servidor suspendido	El administrador de sistemas ha suspendido temporalmente el WebSEAL Server. No se gestionarán peticiones hasta que el administrador vuelva a poner en servicio el servidor.	
1898d439.html	Pérdida de la información de la sesión	La interacción entre el navegador y el servidor consistía en una *sesión permanente* con un servidor principal conectado (junction) que ya no responde. WebSEAL requiere un servicio situado en este servidor para llevar a cabo la petición. Consulte el apartado “Mantenimiento de un estado (opción -s)” en la página 203.	
1898d7af.html	El programa CGI no se ha ejecutado correctamente	Un programa CGI no ha podido ejecutarse correctamente.	
default.html	Error del servidor	WebSEAL no ha podido ejecutar la petición debido a un error inesperado.	500

Soporte de macro

Se dispone de las siguientes macros para utilizarlas en una página de error de HTML personalizada. Las macros sustituyen dinámicamente la información adecuada disponible.

Macro	**Descripción**
ERROR_CODE	El valor numérico del código de error.
ERROR_TEXT	El texto asociado a un código de error en el catálogo de mensajes.
METHOD	El método de HTTP solicitado por el cliente.
URL	El URL solicitado por el cliente.
HOSTNAME	El nombre completo del sistema principal.
HTTP_BASE	El URL de HTTP básico del servidor `http://` *`sistpral`*`:`*`puertatcp`*`/`
HTTPS_BASE	El URL de HTTPS básico del servidor: `https://` *`sistpral`*`:`*`puertassl`*`/`
REFERER	El valor de la cabecera de referencia procedente de la petición o `Desconocido` (si no hay ninguno).
BACK_URL	El valor de la cabecera de referencia procedente de la petición o / (si no hay ninguno).
BACK_NAME	El valor `BACK` si hay una cabecera de referencia en la petición o el valor `HOME` si no la hay.

Capítulo 15. WebSEAL: administración de Smart Junction

WebSEAL puede funcionar como un servidor Web autónomo o como un servidor de conexiones (junction) que proporciona servicios de autentificación y de autorización para servidores principales de aplicaciones. La principal aportación de WebSEAL es su posibilidad de integrar y proteger recursos adicionales de la Web en servidores principales de aplicaciones. WebSEAL integra y protege los recursos de la Web utilizando la tecnología Smart Junction.

Este capítulo incluye los siguientes temas:

Presentación de WebSEAL como servidor Smart Junction

Policy Director proporciona servicios de autentificación, autorización y gestión de redes. En una red basada en la Web, estos servicios los proporciona mejor un WebSEAL Server secundario. El WebSEAL Server secundario protege los recursos de la Web localizados en servidores principales de aplicaciones .

La conexión entre un WebSEAL Server y un servidor principal se conoce como *Smart Junction* o conexión (junction). Utilice una conexión (junction) para combinar los espacios físicos de la Web de WebSEAL y los servidores principales para crear una sola representación lógica del espacio de la Web.

El cliente nunca necesita conocer la ubicación física de un recurso de la Web. WebSEAL convierte las direcciones de URL lógicos en las direcciones físicas que el servidor principal espera. Puede trasladar objetos de la Web de servidor en servidor sin que ello afecte a la forma en que el cliente accede a dichos objetos.

Como servidor de conexiones (junction), WebSEAL puede realizar comprobaciones de autentificación y autorización en todas las peticiones antes de pasarlas a un servidor principal. Las conexiones (junctions), proporcionan un entorno seguro y escalable que permite equilibrar la carga, proporciona una disponibilidad superior y determina las posibilidades de gestión—todo ello realizado de forma transparente para los clientes. La gestión centralizada del espacio de nombres resulta ventajosa para los administradores.

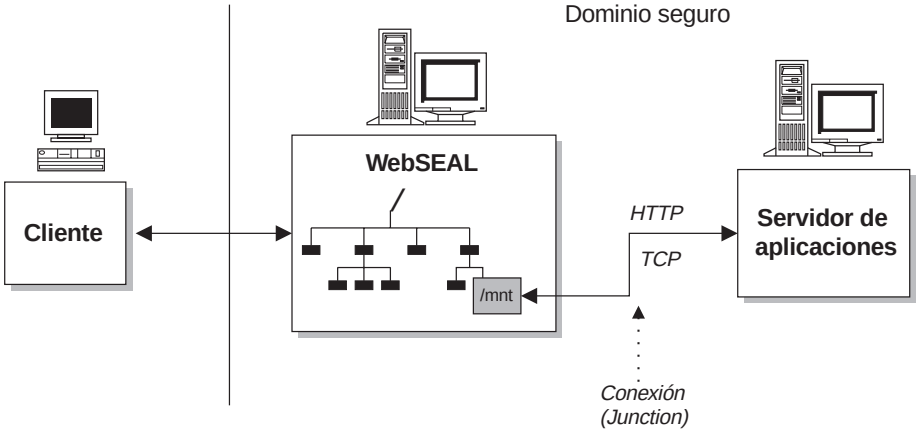
La mayoría de servidores Web comerciales de la Web no tienen la posibilidad de definir un espacio de nombres lógico de la Web. Su control de accesos se conecta al

archivo físico y a la estructura de directorios. Las Smart Junction pueden definir de forma transparente un espacio de nombres que refleje la estructura organizativa en vez de la máquina física y la estructura de directorios que se encuentra normalmente en los servidores Web estándar.

Las conexiones Smart Junction también permiten crear soluciones de conexión propias. Una configuración de conexión propia permite a un usuario acceder a un recurso, independientemente de la ubicación del recurso, utilizando únicamente un inicio de sesión inicial. Cualquier otra solicitud de inicio de sesión procedente de los servidores principales se gestionará de forma transparente para el usuario.

Qué son las conexiones Smart Junction

Una conexión *Smart Junction* es una conexión física TCP/IP entre un WebSEAL Server secundario y un servidor de principal de aplicaciones. El servidor principal puede ser otro WebSEAL Server o un servidor de aplicaciones de terceros. El espacio de la Web del servidor principal de aplicaciones se *conecta* con el WebSEAL Server en un *punto de conexión Smart Junction* (punto de montaje) del espacio de la Web de WebSEAL.

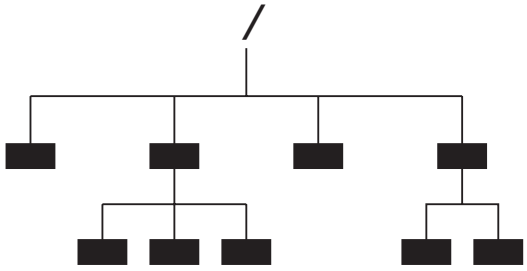


Una Smart Junction permite a WebSEAL proporcionar servicios de protección en nombre del servidor principal de aplicaciones. El servidor principal necesita de un control de accesos estricto para sus objetos. Cuando requiere ese control, deben realizarse otros pasos de configuración para describir el espacio de la Web de terceros al servicio de seguridad de Policy Director.

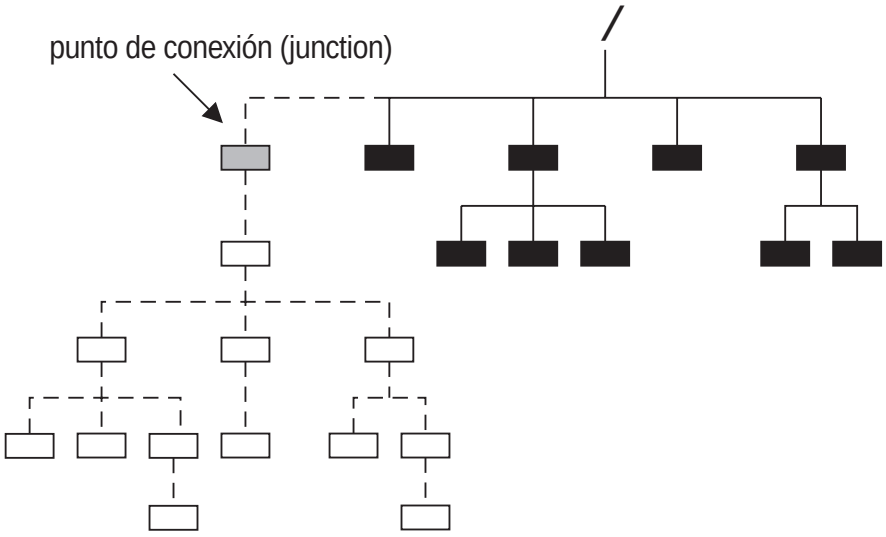
Cuando se configura adecuadamente, WebSEAL protege sus propios recursos y los recursos del servidor conectado (junction) efectuando servicios de seguridad como, por ejemplo, la autentificación, autorización y auditoría.

Las conexiones Smart Junction tienen el valor añadido de combinar de forma lógica el espacio de la Web de un WebSEAL Server con el espacio de la Web de un servidor principal. Las conexiones junction entre servidores que operan conjuntamente dan como resultado un solo espacio de la Web distribuido que no presenta problemas y es transparente para los usuarios.

Un espacio de la Web unificado simplifica la gestión de todos los recursos para el administrador del sistema. También presenta otras ventajas administrativas como, por ejemplo, la escalabilidad, el equilibrio de la carga y una alta disponibilidad.



Espacio de la web de WebSEAL



Espacio de la web combinado:
WebSEAL más servidor conectado (junction)

Las conexiones Smart Junction son una importante herramienta que permite el crecimiento del sitio Web. Estas conexiones permiten responder al aumento de peticiones en un sitio Web conectando servidores adicionales.

Conexiones Smart Junction y escalabilidad del sitio Web

Utilice conexiones Smart Junction para crear un sitio Web escalable. Cuando las peticiones de un sitio Web aumenten, podrá añadir fácilmente más servidores para ampliar la capacidad del sitio. Puede desear añadir más servidores por los siguientes motivos:

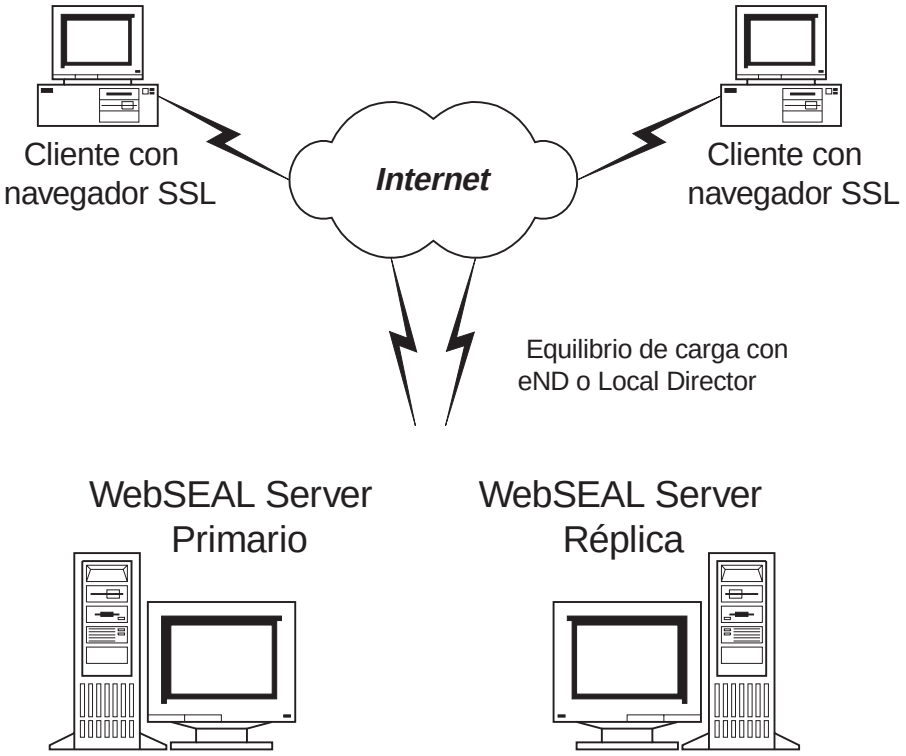
- Para ampliar el sitio con más contenidos
- Para duplicar el contenido existente a fin de equilibrar la carga, ignorar anomalías y tener una gran disponibilidad

Reproducción de WebSEAL Servers secundarios

El soporte de conexiones Junction para servidores principales empieza con un WebSEAL Server secundario como mínimo. Las reproducciones de WebSEAL Servers secundarios permiten equilibrar la carga en el sitio Web en los periodos en

que la demanda es alta. Una aplicación (como Policy Director eND o Cisco Local Director) gestiona el mecanismo de equilibrio de carga.

La reproducción de servidores secundarios también proporciona al sitio Web la posibilidad de ignorar una anomalía. Si un servidor falla por algún motivo, el resto de servidores reproducidos continuará proporcionando acceso al sitio Web. El equilibrio de la carga y la posibilidad de ignorar anomalías se traducen en una alta disponibilidad para los usuarios del sitio Web.



Hay dos puntos que deben recordarse sobre la reproducción de WebSEAL Servers secundarios:

- Cada servidor debe contener una copia exacta del espacio de la Web.
- Para que la autentificación sea coherente, debe hacerse una réplica de la base de datos de contabilidad.

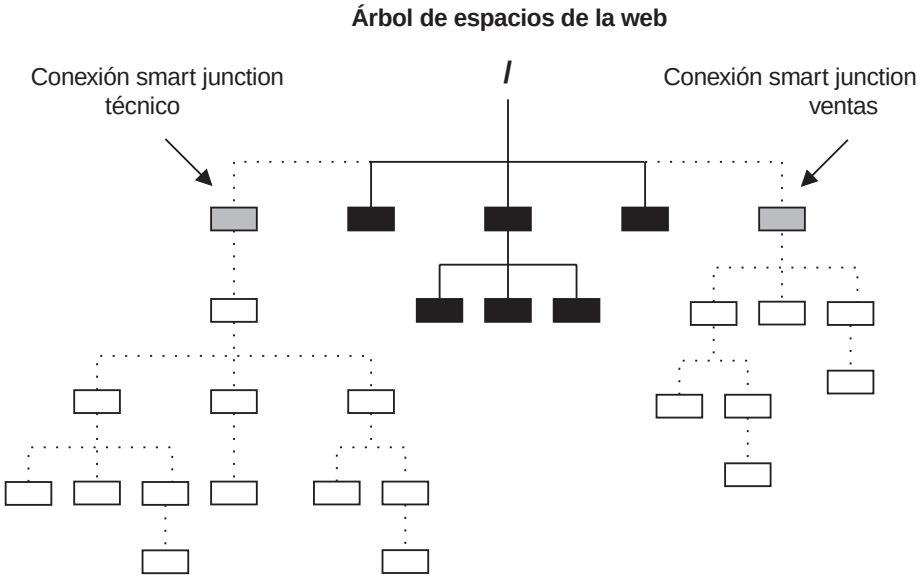
Policy Director Authorization Service reproduce automáticamente la información de la base de datos de autorizaciones cuando es necesario.

Soporte de servidores principales

El WebSEAL Server propiamente dicho, uno o varios servidores principales, o una combinación del WebSEAL Server y un servidor principal, pueden atender al contenido del sitio Web. El soporte de Smart Junction para servidores principales permite ampliar el sitio Web mediante contenidos y recursos adicionales.

Cada uno de los servidores principales debe conectarse a un punto de conexión Smart Junction (de montaje). A medida que la demanda de contenidos y recursos adicionales crece, añada más servidores utilizando conexiones Smart Junction. Este marco proporciona una solución para redes que hayan efectuado una gran inversión en servidores Web de terceros.

El siguiente diagrama explica cómo las Smart Junctions proporcionan un espacio de la Web lógico y unificado. Dicho espacio de la Web es transparente para el usuario y permite una gestión centralizada.



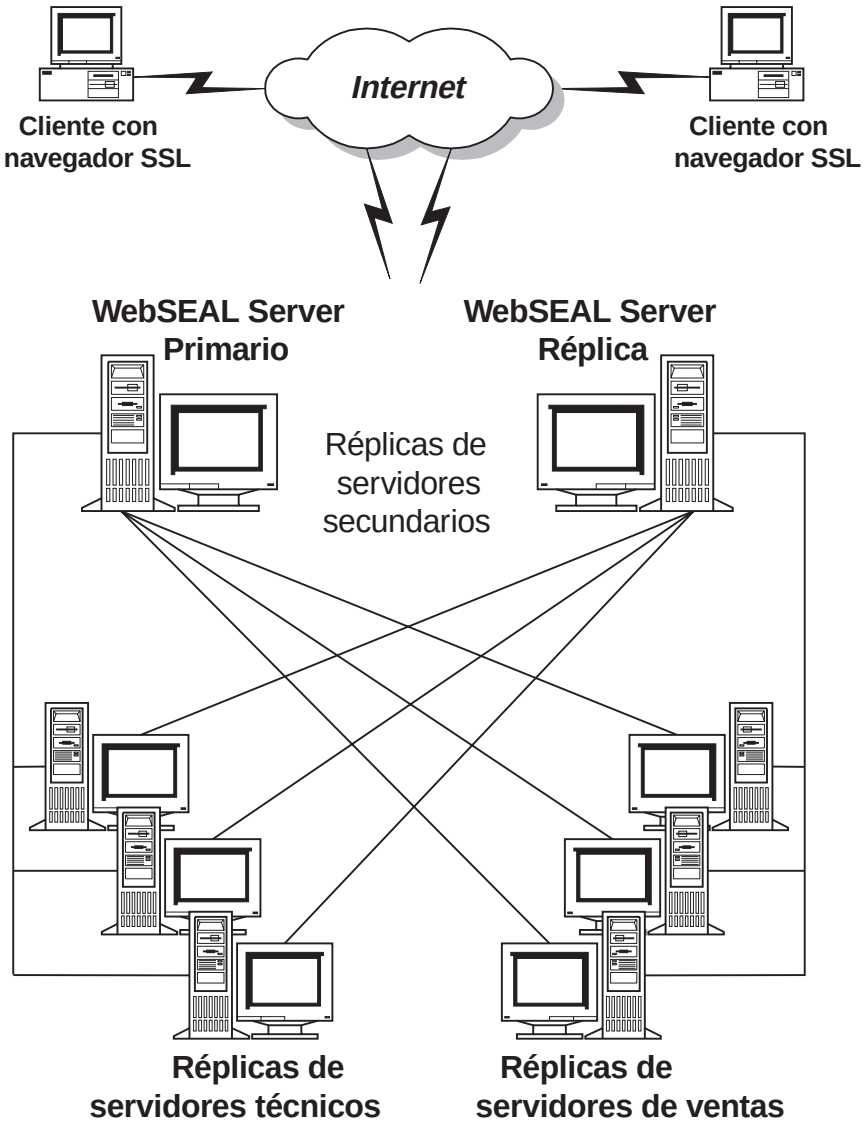
Los servidores principales reproducidos se conectan con Smart Junction al mismo punto de conexión Smart Junction, como se explica en el apartado “Reproducción de servidores principales”.

Reproducción de servidores principales

Para ampliar las funciones de escalabilidad para una configuración de servidor principal, puede reproducir los servidores principales. Como en el caso de los servidores secundarios, los servidores principales reproducidos deben contener espacios de la Web que sean imágenes especulares los unos de los otros.

WebSEAL equilibra la carga a través de servidores reproducidos utilizando un algoritmo de planificación “menos ocupado”. WebSEAL también ignora correctamente la anomalía cuando un servidor está desactivado y empieza a utilizar de nuevo el servidor restaurado.

Si la aplicación principal requiere que el estado se mantenga a lo largo de varias páginas, puede utilizar conexiones Junction permanentes. Estas *conexiones permanentes* aseguran que cada sesión vuelva al mismo servidor principal. Consulte el apartado “Mantenimiento de un estado (opción -s)” en la página 203.



Resumen de tareas para crear conexiones Smart Junction

Puede crear los siguientes tipos de conexiones Smart Junction:

- Policy Director a terceros; conexión TCP
- Policy Director a terceros; conexión SSL
- Policy Director a sistema de archivos local

Los siguientes pasos resumen las tareas que es necesario realizar para conectar (junction) un espacio de la Web de un servidor principal de aplicaciones al espacio de la Web de WebSEAL:

1. Decida dónde desea conectar con Smart Junction (montar) los servidores adicionales en el espacio de la Web de WebSEAL.
2. Determine qué condiciones de seguridad requiere para asegurar la integridad de la red.

Control de accesos flexible

Para proporcionar un control de accesos flexible:

1. Cree una conexión Smart Junction entre el espacio de la Web aplicaciones principales de terceros y el WebSEAL Server secundario utilizando el programa de utilidad **junctioncp** de Policy Director.
2. Coloque una plantilla de política (ACL) adecuada en el punto de conexión Smart Junction para proporcionar un control general al servidor principal.

Control de accesos estricto

Para proporcionar un control de accesos estricto:

1. Cree una conexión Smart Junction entre el espacio de la Web de aplicaciones principales de terceros y el WebSEAL Server secundario utilizando el programa de utilidad **junctioncp**.

   WebSEAL no puede *ver* y comprender automáticamente un sistema de archivos de terceros. Deberá informar a WebSEAL del espacio de nombres de terceros utilizando **query_contents**. Esta aplicación especial hace un inventario del espacio de la Web de terceros e informa de su estructura a WebSEAL.
2. Copie el programa **query_contents** en el servidor de terceros.
3. Utilice Management Console para aplicar las plantillas de políticas (ACL) a los objetos pertinentes del espacio de la Web unificado.

Directrices para la creación de conexiones Smart Junction

Las siguientes directrices resumen las normas para conexiones Smart Junction:

- Se puede añadir una conexión Smart Junction en cualquier lugar del espacio de nombres primario de WebSEAL.
- Se pueden conectar (junction) múltiples réplicas de servidores en un mismo punto de montaje (punto de conexión Smart Junction).
- Si se montan varias réplicas de servidores en el mismo punto de conexión Smart Junction, deben ser del mismo tipo (TCP o SSL).
- No se pueden encadenar servidores de terceros (como Policy Director — servidor de terceros — servidor de terceros).

Control de accesos y privilegios administrativos

Por omisión, la cuenta del administrador de célula tiene todos los derechos para todo el espacio de la Web y esto incluye los servidores conectados (junction). El administrador de un servidor conectado (junction) sólo mantiene el espacio de la Web para dicho servidor. Cuando es necesario, el administrador puede suprimir privilegios administrativos del servidor desde el administrador de célula.

Policy Director hereda la ACL a través de conexiones Smart Junction con servidores de terceros.

Utilización de junctioncp para gestionar conexiones Smart Junction

Utilice el programa de utilidad **junctioncp** para llevar a cabo todas las tareas de gestión de conexiones (junction):

- Crear un nuevo punto de conexión Smart Junction
- Añadir un servidor al punto de conexión Smart Junction
- Eliminar un servidor del punto de conexión Smart Junction
- Eliminar un punto de conexión Smart Junction
- Visualizar una lista de puntos de conexión Smart Junction
- Visualizar los detalles de una conexión (junction)

El programa de utilidad **junctioncp** proporciona un indicador de mandatos interactivo desde donde pueden efectuarse las tareas de conexión.

Antes de iniciar **junctioncp**, debe iniciar la sesión con un dominio seguro como usuario administrador. Puede utilizar dce_login en un entorno UNIX o Windows. Puede utilizar netseat_login en un entorno Windows.

Inicie el programa de utilidad **junctioncp** con la opción **-e** para especificar el servidor (nombre del sistema principal) donde desea efectuar las tareas de conexión (junction). Se visualizará el indicador de mandatos **junctioncp**.

Por ejemplo:

UNIX:

```
#
# junctioncp -e nombre-servidor

junctioncp>
```

Windows:

```
junctioncp -e <nombre-servidor>

junctioncp>
```

Utilización de mandatos junctioncp

Con **junctioncp** se dispone de los siguientes mandatos:

Mandato	Descripción
create	Crear una nueva conexión Smart Junction para un servidor inicial.
add	Añadir servidores adicionales con un punto de conexión Smart Junction existente.
remove	Eliminar un servidor de un punto de conexión Smart Junction.
delete	Eliminar el punto de conexión Smart Junction.
list	Listar todos los puntos de conexión Smart Junction del servidor.
show	Visualizar los detalles de una conexión Smart Junction.
help	Listar los mandatos de **junctioncp**.
help *mandato*	Visualizar ayuda detallada de un mandato específico de **junctioncp**.
exit	Salir del programa de utilidad **junctioncp**.

En el apartado “Creación de una nueva conexión Smart Junction para un servidor inicial” están explicados estos mandatos y las opciones relacionadas con los mismos.

Creación de una nueva conexión Smart Junction para un servidor inicial

Operación: Crea un nuevo punto de conexión Smart Junction y conecta un servidor inicial.

Sintaxis: `create -t` *`tipo`* `-h` *`nombre-sistema-principal opciones punto-conexión-Smart-Junction`*

tipo

Uno de estos: • **tcp** • **ssl** • **local**		*Necesario.* Define el tipo de conexión Smart Junction. Utilice **tcp** para servidores principales de terceros. Cuando se utiliza la opción **ssl**, la puerta TCP por omisión cambia de 80 a 443. Consulte el apartado “Creación de conexiones Smart Junction SSL seguras” en la página 204.
opciones		
	Opciones de conexión Smart Junction TCP y SSL (Utilícelas con **-t tcp** o **-t ssl**)	
	-2	Fuerza la comunicación con el servidor principal utilizando únicamente SSL Versión 2. Consulte el apartado “Creación de conexiones Smart Junction SSL seguras” en la página 204.
	-b *valor-ba* Uno de estos: • **filter** (por omisión) • **ignore** • **supply** • **gso**	Define la forma en que WebSEAL Server pasa la información de autentificación a los servidores principales. Consulte el apartado “Suministro de información de autentificación a servidores conectados con Smart Junction” en la página 209.
	-c	Inserta la identidad de Policy Director en cabeceras HTTP. Consulte el apartado “Inserción de información de la identidad del cliente (opción -c)” en la página 203.
	-i	Hace que WebSEAL Server trate los URL como insensibles a mayúsculas y minúsculas. Consulte el apartado “Soporte de URL insensibles a mayúsculas y minúsculas (opción -i)” en la página 201.
	-h *nombre sistema principal*	*Necesario.* Define el nombre de sistema principal del servidor principal de destino (DNS). Alternativamente, puede suministrar su dirección IP.
	-p *puerta*	Define la puerta TCP del servidor principal de terceros. El valor por omisión es 80 para conexiones Smart Junction TCP; 443 para conexiones Smart Junction SSL.
	-q *url*	Define el URL para el script **query_contents**. Policy Director busca **query_contents** en /cgi_bin/. Cuando este directorio es diferente o se ha dado un nuevo nombre al archivo **query_contents**, utilice esta opción para indicar a WebSEAL el nuevo URL del archivo. Cuando cree una conexión Smart Junction para el servidor de terceros Win32, utilice esta opción **-q**. Consulte el apartado “Configuración de una conexión Smart Junction para encontrar query_contents” en la página 219.
	-s	Indica que la conexión Smart Junction debe tener soporte para aplicaciones permanentes. Por omisión, las conexiones Smart Junction no son *permanentes*. Consulte el apartado “Mantenimiento de un estado (opción -s)” en la página 203.

	-T *recurso*	Define el nombre del recurso de la aplicación para Credenciales de recursos GSO. Necesario y utilizado únicamente con la opción **-b gso**. Consulte el apartado “Integración de la conexión propia de WebSEAL y GSO” en la página 213.
	-v *nombre sistema principal*	Define el nombre del sistema principal virtual del servidor.
	-w	Define el soporte del sistema de archivos Win32. Consulte el apartado “Inhabilitación de la forma de nombre de archivo corto (opción -w)” en la página 202.
	Opciones de conexiones Smart Junction locales y DFS (utilícelas con **-t dfs** o **local**)	
	-d *dir*	Define el sistema de archivos distribuido (DFS) o el directorio local que debe conectarse (junction). Necesario.
punto-conexión-Smart-Junction		
	Define la ubicación en el espacio de nombres de WebSEAL donde va a crearse la conexión Smart Junction.	

Adición de otro servidor a una conexión Smart Junction existente

Operación: Añade otro servidor a un punto de conexión Smart Junction existente.

Sintaxis: `add -h` *`nombre-sistema-principal opciones punto-conexión-Smart-Junction`*

opciones		
	Opciones de conexión Smart Junction TCP y SSL	
	-i	Hace que WebSEAL Server trate los URL como insensibles a mayúsculas y minúsculas. Consulte el apartado “Soporte de URL insensibles a mayúsculas y minúsculas (opción -i)” en la página 201.
	-h *nombre sistema principal*	*Necesario.* Define el nombre del sistema principal del servidor principal de destino (DNS). Alternativamente, puede suministrar su dirección de IP.
	-p *puerta*	Define la puerta TCP del servidor principal de terceros. El valor por omisión es 80 para conexiones Smart Junction TCP; 443 para conexiones Smart Junction SSL.
	-q *url*	Define el URL para el script **query_contents**. Policy Director busca **query_contents** en /cgi_bin/. Cuando este directorio es diferente o se ha dado un nuevo nombre al archivo **query_contents**, utilice esta opción para indicar a WebSEAL el nuevo URL del archivo.
	-v *nombre sistema principal*	Define el nombre del sistema principal virtual del servidor.

	-w	Define el soporte del sistema de archivos Win32. Consulte el apartado “Inhabilitación de la forma de nombre de archivo corto (opción -w)” en la página 202.
punto-conexión-Smart-Junction		
	Añade un servidor a un punto de conexión Smart Junction existente.	

Utilización de otros mandatos de junctioncp

En los apartados “Creación de una nueva conexión Smart Junction para un servidor inicial” en la página 198 y “Adición de otro servidor a una conexión Smart Junction existente” en la página 200) están explicados los mandatos **junctioncp create** y **junctioncp add**. La siguiente tabla lista los demás mandatos de **junctioncp** disponibles:

Mandato	Descripciones
remove	**Operación:** Elimina un servidor principal de un punto de conexión Smart Junction. **Sintaxis:** `remove -i` *`id-servidor punto-conexión-Smart-Junction`* **Opciones: -i** *id-servidor* Identificación del servidor que se va a eliminar. Utilice el mandato show para determinar el ID de un servidor determinado.
delete	**Operación:** Elimina un punto de conexión Smart Junction. **Sintaxis:** `delete` *`punto-conexión-Smart-Junction`*
show	**Operación:** Visualiza los detalles de una conexión Smart Junction. **Sintaxis:** `show` *`punto-conexión-Smart-Junction`*
list	**Operación:** Lista todas las conexiones Smart Junction. **Sintaxis:** `list`
help	**Operación:** Visualiza la lista de los mandatos de **junctioncp**. **Sintaxis:** `help`
help *mandato*	**Operación:** Visualiza información sobre un mandato de **junctioncp** específico, incluidas las opciones disponibles. **Sintaxis:** `help` *`mandato`*
exit	**Operación:** Sale del programa de utilidad **junctioncp** y vuelve al indicador del sistema operativo. **Sintaxis:** `exit`

Soporte de URL insensibles a mayúsculas y minúsculas (opción -i)

Utilice la opción **-i** cuando esté conectando (junction) servidores de terceros para indicar que WebSEAL tratará los URL como insensibles a mayúsculas y minúsculas. Esto significa que el servidor no hará diferencias entre los caracteres que estén en mayúsculas y los que estén en minúsculas cuando analice el URL. Por omisión, los servidores son normalmente sensibles a las mayúsculas y minúsculas.

Aunque la mayoría de servidores HTTP tiene soporte para la especificación de HTTP que define los URL como sensibles a las mayúsculas y minúsculas, algunos servidores HTTP tratan los URL como insensibles a las mayúsculas y minúsculas.

Por ejemplo, en servidores insensibles a mayúsculas y minúsculas, pueden verse dos URL como un mismo URL:

```
http://server/sales/index.htm
```

```
http://server/SALES/index.HTM
```

Este comportamiento requiere que Policy Director coloque los mismos controles de acceso (ACL) en ambos URL. Por omisión, Policy Director trata los URL como sensibles a las mayúsculas y minúsculas cuando aplica controles de acceso. Cuando se conecta con Smart Junction un servidor de terceros con la opción **-i**, WebSEAL trata los URL que se dirigen a dicho servidor como insensibles a mayúsculas y minúsculas.

Inhabilitación de la forma de nombre de archivo corto (opción -w)

La finalidad de esta operación es restringir el control de accesos a una sola representación de objeto. No permitir la existencia de *puertas traseras* que eludan el mecanismo de seguridad.

WebSEAL efectúa comprobaciones de seguridad en peticiones de clientes de servidores principales basadas en las vías de acceso a archivos especificados en el URL. En esta comprobación de seguridad podría producirse una situación comprometida porque los sistemas de archivos de Win32 proporcionan dos métodos distintos para acceder a nombres de archivos largos.

El primer método reconoce todos el nombre de archivo (`abcdefghijkl.txt`). El segundo método utiliza el formato antiguo de nombres de archivo 8.3 (`abcdef~1.txt`) para que pueda haber compatibilidad con elementos anteriores.

La opción **-w** del mandato **junctioncp** rechaza el formato de nombres de archivos 8.3. Un usuario no puede evitar una ACL explícita en un nombre de archivo largo utilizando el formato corto (8.3) de nombres de archivos. El servidor devuelve un error `403 Prohibido` cuando se entra cualquier formato corto de nombre de archivo.

Windows trata un nombre de archivo “foo.” igual que trataría el nombre de archivo “foo” sin el punto final. La opción **-w** elimina los puntos finales de los nombres de archivos de un URL antes de enviar la petición al servidor principal. Policy Director basa las comprobaciones de ACL en el nombre del archivo—sin el punto final.

Nota: La opción **-i** trata el problema de la insensibilidad a mayúsculas y minúsculas de Win32 (`abced.txt` = `AbCdE.txt`).

Ejemplo:

En Windows NT 4.0, puede acceder a las siguientes vías de acceso al archivo \Archivos de programa\ibm corp\readme.txt como sigue:

1. \Archivos de programa\ibm corp.\readme.txt
2. \Archivos de programa\ibm corp\readme.txt
3. \Archiv~1\ibm~2\readm~3.txt

El ejemplo 1 de arriba describe el efecto de la “insensibilidad a mayúsculas y minúsculas”. La opción **-i** (no la opción **-w**) trata de este efecto.

El ejemplo 2 describe la forma en que Windows NT ignora un punto final de extensión.

El ejemplo 3 describe la forma en que Windows NT crea un alias para que exista compatibilidad con Disk Operating System (DOS). El alias no debe contener espacios en los nombres de archivos y debe ajustarse al formato 8.3.

La opción **-w** trata las posibles deficiencias en la seguridad ilustradas por los ejemplos 2 y 3. La opción **-w** indica que Policy Director ignorará los puntos finales. Esta opción también indica que Policy Director desautoriza el acceso a nombres de archivos acortados que contengan un carácter de tilde (~) en URL solicitados para el servidor conectado con Smart Junction.

Mantenimiento de un estado (opción -s)

La mayoría de aplicaciones habilitadas para la Web mantienen un *estado* a través de una secuencia de peticiones HTTP contenida en cada sesión de cliente. Por ejemplo, el estado se utiliza para:

- Efectuar un seguimiento del proceso de un usuario a través de los campos en forma de entrada de datos que genera un programa CGI
- Mantener el contexto de un usuario cuando se efectúa una serie de consultas a la base de datos
- Mantener una lista de elementos en una aplicación de compras en línea en la que un usuario examina al azar y selecciona artículos para comprarlos

Los servidores que ejecutan aplicaciones preparadas para la Web pueden reproducirse, como cualquier servidor, para mejorar el rendimiento gracias al reparto de la carga. Policy Director Server puede proporcionar una conexión Smart Junction para esos servidores reproducidos. Si es así, deberá asegurar que todas las peticiones contenidas en una sesión de cliente se envían al servidor correcto. También deberá asegurar que todas las peticiones no se distribuyen entre los servidores reproducidos según las normas de equilibrio de carga.

Por omisión, Policy Director equilibra la carga del servidor distribuyendo peticiones entre todos los servidores reproducidos. Policy Director utiliza un algoritmo de “menos ocupado”.

Para alterar temporalmente ese equilibrio de carga y crear una *conexión Smart Junction permanente*, utilice el mandato **junctioncp** con la opción **-s**. La conexión Smart Junction permanente asegura que las peticiones de clientes se envían a un mismo servidor durante toda la sesión.

Inserción de información de la identidad del cliente (opción -c)

La opción **-c** permite insertar información específica de Policy Director sobre la identidad y la pertenencia a un grupo del cliente en las cabeceras de las peticiones HTTP. Las peticiones HTTP se destinan a servidores de terceros con conexiones Smart Junction. Las cabeceras HTTP específicas de Policy Director permiten a las aplicaciones de servidores de terceros conectados con Smart Junction realizar acciones específicas de los usuarios. Las acciones específicas de usuarios se basan en la identidad del Policy Director del cliente.

La información de cabecera HTTP debe adoptar el formato de variable de entorno para que la utilice un servicio del servidor principal. La información de cabecera adopta el formato de una variable de entorno CGI sustituyendo todos los guiones (-) por signos de subrayado (_) y colocando “HTTP” al principio de la cadena de caracteres. El valor de la cabecera HTTP pasa a ser el valor de la nueva variable de entorno.

Las entradas de cabecera HTTP específicas de Policy Director incluyen:

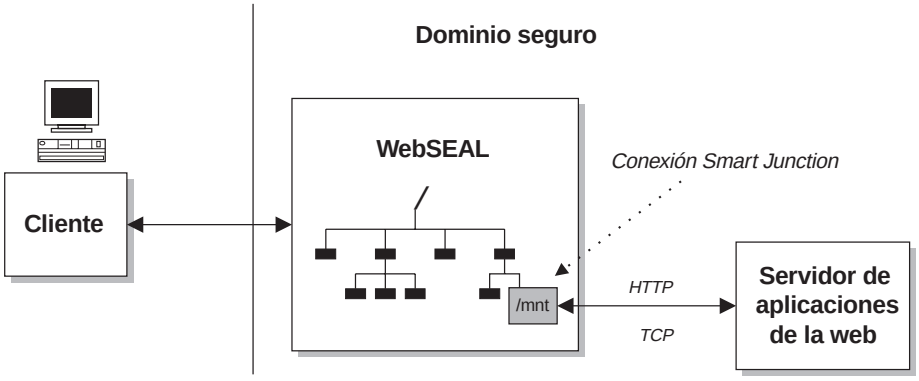
cabeceras HTTP específicas de Policy Director	Formato de variable de entorno CGI	Descripción
iv-user	HTTP_IV_USER	El nombre del cliente. Por omisión es **Unauthenticated** cuando el cliente no está autentificado (es desconocido).
iv-groups	HTTP_IV_GROUPS	Una lista grupos a los que pertenece el cliente. Consta de entradas separadas por espacios.
iv-creds	HTTP_IV_CREDS	Estructura de datos opacos codificados que representa una credencial de recurso de Policy Director. Se utiliza junto con la API de autorizaciones de Policy Director. Si desea ver información más detallada, consulte el manual *Policy Director Programmer’s Guide and Reference.*

Las entradas de la cabecera HTTP están disponibles para los programas CGI como variables de entorno HTTP_IV_USER, HTTP_IV_GROUP y HTTP_IV_CREDS. Para otros productos de infraestructura de aplicaciones, consulte la documentación del producto donde encontrará las instrucciones pertinentes para la extracción de cabeceras de peticiones HTTP.

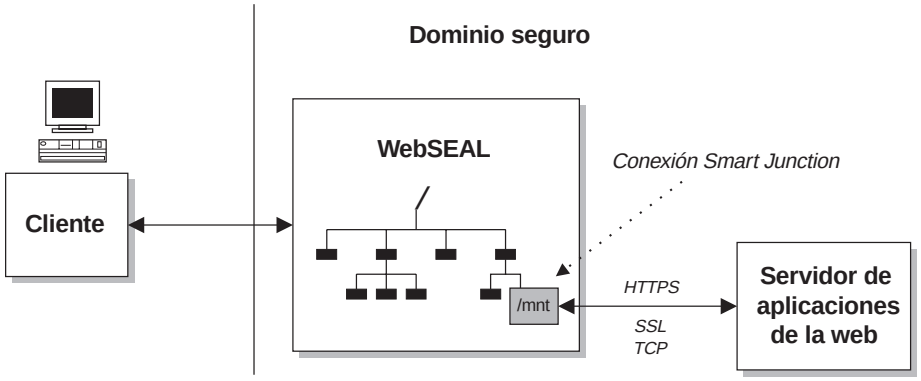
Creación de conexiones Smart Junction SSL seguras

WebSEAL tiene soporte para conexiones Smart Junction TCP (HTTP) estándar y SSL (HTTPS) seguras entre WebSEAL y los servidores principales. Las conexiones Smart Junction SSL funcionan exactamente igual que las conexiones Smart Junction TCP, con el valor añadido de que todas las comunicaciones entre WebSEAL y el servidor principal están cifradas.

La siguiente figura presenta una conexión Smart Junction TCP (HTTP) que no es segura.



La siguiente figura presenta una conexión Smart Junction SSL (HTTPS) segura.



La conexión Smart Junction entre WebSEAL y el servidor principal es independiente del tipo de conexión (y de su nivel de seguridad) entre el cliente y el WebSEAL Server.

Las conexiones Smart Junction SSL permiten transacciones seguras de principio a fin del navegador a la aplicación. Utilice SSL para asegurar las comunicaciones desde el cliente a WebSEAL y desde WebSEAL a los servidores principales.

Configuración de una conexión Smart Junction SSL segura

Para el funcionamiento de Smart Junction SSL se requiere que el servidor Web principal esté habilitado para HTTPS.

Para crear una conexión Smart Junction, utilice el programa de utilidad **junctioncp**. El apartado “Utilización de junctioncp para gestionar conexiones Smart Junction” en la página 197 describe detalladamente el programa de utilidad **junctioncp**.

Para crear una conexión Smart Junction SSL segura y añadir un servidor inicial, utilice el mandato **junctioncp create**. El siguiente ejemplo, ilustra la sintaxis del mandato create para crear una conexión Smart Junction SSL segura:

```
junctioncp> create -t ssl [-2] -h nombre-sistema-principal
[-p  puerta] punto-conexión-Smart-Junction
```

La opción **-2** fuerza a Policy Director a comunicarse con el servidor principal utilizando únicamente SSL Versión 2.

Normalmente, Policy Director negocia automáticamente la versión del protocolo SSL (Versión 2 o Versión 3). Policy Director introdujo la opción **-2** porque algunos servidores IIS hacían que Policy Director no respondiese correctamente cuando intentaba negociar con SSL Versión 3. Cuando se produce esto, el montaje no se ejecuta correctamente. Al forzar la utilización de la Versión 2 el problema se resuelve.

Revisión de ejemplos de conexiones Smart Junction SSL

Sistema principal con conexión Smart Junction sales.ibm.com en el punto de conexión Smart Junction /sales que utiliza el protocolo SSL:

```
create -t ssl -h sales.ibm.com /sales
```

Sistema principal con conexión Smart Junction admin.ibm.com en el punto de conexión Smart Junction /admin que utiliza únicamente el protocolo SSL Versión 2:

```
create -t ssl -2 -h admin.ibm.com /admin
```

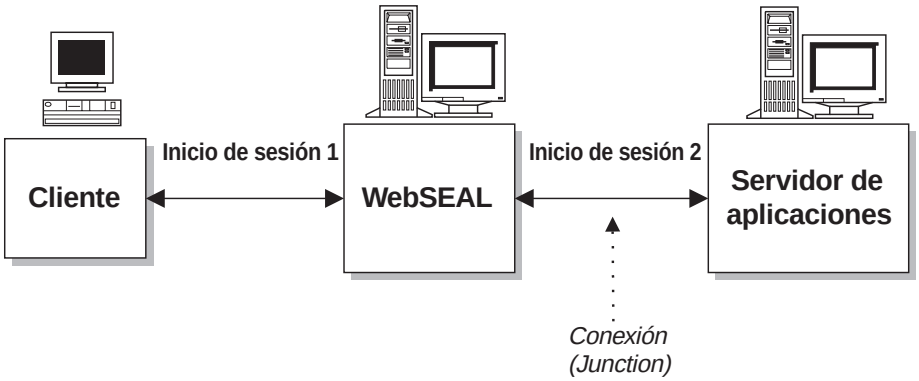
Nota: En los dos ejemplos anteriores, la opción **-t ssl** indica la puerta por omisión 443.

Sistema principal con conexión Smart Junction travel_svr en la puerta 4343 en el punto de conexión Smart Junction /travel que utiliza el protocolo SSL:

```
create -t ssl -p 4343 -h travel_svr  /travel
```

Utilización de la solución de conexión propia de Policy Director

Cuando se localiza un recurso protegido en un servidor principal, un cliente que solicite dicho recurso puede tener que realizar varios inicios de sesión. Los múltiples inicios de sesión incluyen uno para el WebSEAL Server y uno para cada servidor principal. Es probable que cada inicio de sesión requiera distintas identidades de inicio de sesión.



El problema de la administración y mantenimiento de varias identidades de inicio de sesión puede solucionarse con el mecanismo de conexión propia. Una solución de conexión propia permite a un usuario acceder a un recurso, independientemente de la ubicación del recurso, utilizando únicamente un inicio de sesión inicial. Cualquier otra solicitud de inicio de sesión procedente de los servidores principales se gestionará de forma transparente para el usuario.

El administrador de seguridad de la red debe tomar tres decisiones importantes cuando configure un mecanismo de conexión propia para Policy Director:

1. ¿Necesitan los servidores principales información de autentificación?

   WebSEAL utiliza la cabecera de *autentificación básica* de HTTP para transmitir información de autentificación.
2. Si los servidores principales necesitan información de autentificación ¿de dónde procede la misma? (¿Qué información coloca WebSEAL en la cabecera HTTP?)
3. ¿Es necesario que la conexión entre WebSEAL y los servidores principales sea segura? (¿Conexión Smart Junction TCP o SSL?)

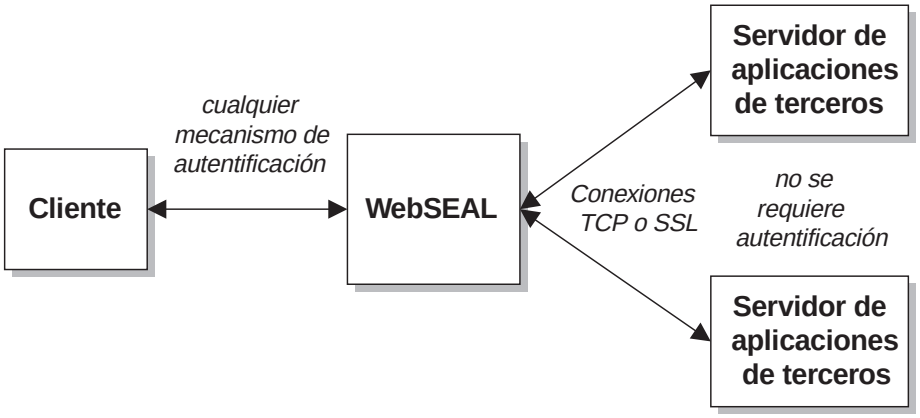
Las siguientes secciones examinan algunas de las configuraciones de conexión propia típicas de WebSEAL.

Servidores principales que no requieren autentificación

Cuando el servidor principal no requiere información de autentificación, se dan las siguientes condiciones:

- No es necesario configurar WebSEAL para enviar información de autentificación a través de la conexión Smart Junction.
- Sólo se puede acceder a servidores principales a través de WebSEAL.
- WebSEAL gestiona la autentificación en nombre de todos los servidores principales.
- Hay también una opción especial para pasar información de la identidad del usuario a los servidores principales a fin de realizar otras acciones de autorización, si es necesario. Esta opción especifica es la opción **-c** del programa de utilidad **junctioncp**.

Consulte el apartado “Sin información de autentificación” en la página 212.

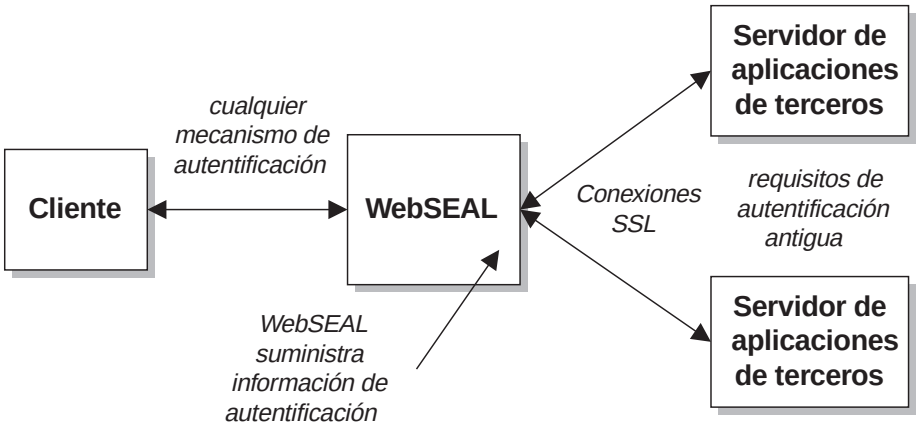


Servidores principales con requerimientos de autentificación antiguos

Cuando el servidor principal contiene mecanismos de autentificación antiguos a los que debe darse soporte, se dan las siguientes condiciones:

- WebSEAL debe configurarse para que suministre la información de autentificación adecuada a los servidores principales.
- Es probable que la información de autentificación proceda de un mecanismo como GSO.

  Consulte el apartado “Integración de la conexión propia de WebSEAL y GSO” en la página 213 .
- Como Policy Director pasa información de autentificación confidencial (nombre de usuario y contraseña) a través de la conexión Smart Junction, la seguridad de dicha conexión es importante. Por lo tanto, Policy Director aconseja la utilización de conexiones Smart Junction SSL.

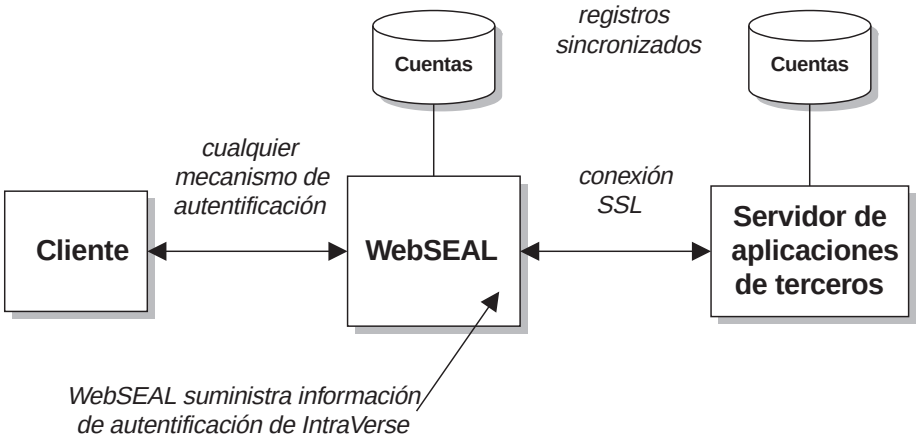


Conexión propia de Policy Director

Cuando el servidor principal requiere información de autentificación de Policy Director, se dan las siguientes condiciones:

- WebSEAL debe configurarse para que suministre a los servidores principales el nombre de usuario y la contraseña contenidos en la petición original del cliente.
- Los servidores principales deben comprender la identidad y la contraseña de Policy Director suministrados en la cabecera HTTP de autentificación básica (basic authentication, BA). Por lo tanto, WebSEAL y los servidores principales deben tener registros de usuarios sincronizados.
- Como Policy Director pasa información de autentificación confidencial (nombre de usuario y contraseña) a través de la conexión Smart Junction, la seguridad de dicha conexión es importante. Policy Director aconseja la utilización de conexiones Smart Junction SSL.

Consulte el apartado “Información de cabecera de BA de cliente original” en la página 211.

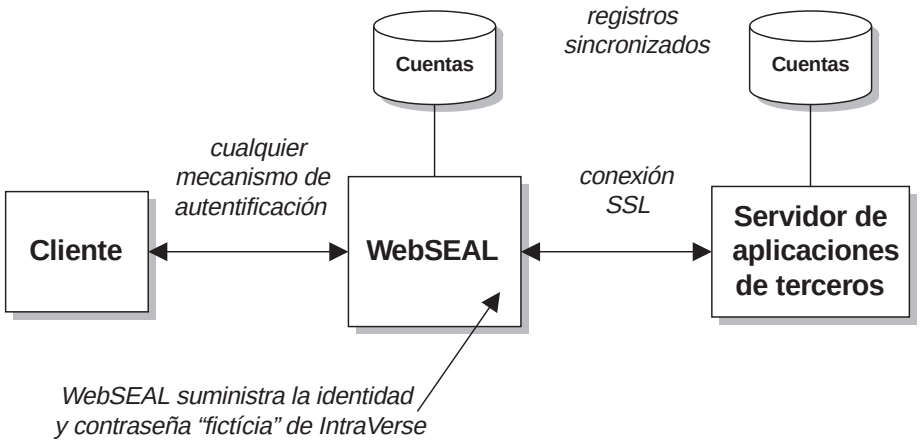


Conexión propia de Policy Director limitada

Se dispone de una conexión propia de Policy Director limitada cuando la cabecera de BA HTTP indica la identidad de Policy Director (nombre del usuario). También se facilita una contraseña estática, genérica. Este marco es el adecuado para una utilización por aplicación-usuario. Esta solución puede resultar ventajosa porque no requiere administración de contraseñas. Se dan las siguientes condiciones:

- WebSEAL debe configurarse para suministre a los servidores principales el nombre de usuario contenido en la petición del cliente original más una contraseña genérica (ficticia).
- Configure la contraseña ficticia en el archivo de configuración iv.conf.
- Los servidores principales deben comprender la identidad de Policy Director facilitada en la cabecera de BA HTTP. Por lo tanto, WebSEAL y los servidores principales deben tener registros de contabilidad sincronizados.
- Como Policy Director pasa información de autentificación confidencial (nombre de usuario y contraseña) a través de la conexión Smart Junction, la seguridad de dicha conexión es importante. Policy Director aconseja la utilización de conexiones Smart Junction SSL.

Consulte el apartado “Identidad y contraseña genérica de Policy Director” en la página 210.



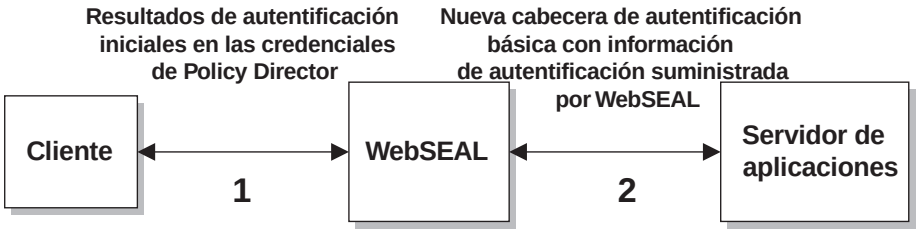
Suministro de información de autentificación a servidores conectados con Smart Junction

Existen varios supuestos en los que puede pasarse información de autentificación de WebSEAL a uno o varios servidores principales. Es el administrador quien debe decidir si se envía o no la información de autentificación que se coloca en la cabecera de autentificación básica HTTP para el servidor principal.

¿Cuál es el origen de esta información de autentificación?

Tras la autentificación inicial entre el cliente y WebSEAL, WebSEAL crea una nueva cabecera de autentificación básica. La petición utiliza esta nueva cabecera durante su recorrido a través de la conexión (junction) hasta llegar al servidor principal. Utilice las opciones que proporciona el programa de utilidad **junctioncp** para indicar la información de autentificación que facilitará la nueva cabecera.

Debe analizar la arquitectura de la red y los requisitos de seguridad y decidir a continuación qué información de cabecera (si la hay) debe pasar por la conexión.

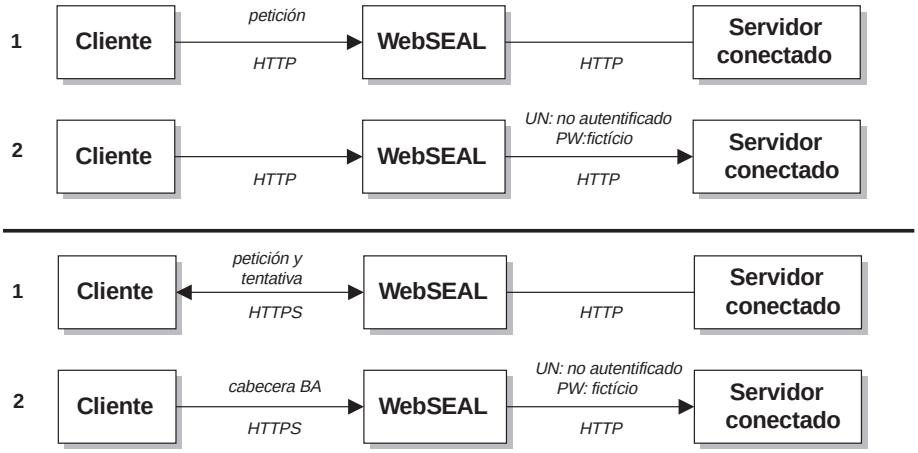


Identidad y contraseña genérica de Policy Director

opción de junctioncp: -b supply

Esta opción indica a WebSEAL que suministre el nombre del usuario de Policy Director autentificado (identidad original del cliente) y una contraseña genérica (ficticia). En este caso no se utiliza la contraseña del cliente original.

En este ejemplo se supone que el servidor principal requiere autentificación de una identidad de Policy Director. Correlacionando un usuario del cliente con un usuario de Policy Director conocido, Policy Director gestiona la autentificación para el servidor principal. Policy Director proporciona también una solución de conexión propia para todo el dominio.



Limitaciones:

Policy Director utiliza la misma contraseña ficticia para todas las peticiones; todos los usuarios tienen la misma contraseña en el registro principal. Si los clientes siempre pasan por WebSEAL para acceder al servidor conectado con Smart Junction, esta solución no presentará ningún problema de seguridad.

Una contraseña genérica elimina la administración de contraseñas y soporta las aplicaciones por usuario. El parámetro **basic_auth_passwd** del archivo de configuración iv.conf establece la contraseña ficticia.

```
basic_auth_passwd = contraseña
```

Como en este ejemplo no existe seguridad a nivel de contraseña, el servidor principal debe confiar implícitamente en WebSEAL para que verifique la legitimidad del cliente.

El servidor también debe comprender la identidad de Policy Director para poder aceptarla. Esto requiere la sincronización del servidor principal con el registro de WebSEAL.

La utilización de la contraseña ficticia común no ofrece ninguna base al servidor principal para que pueda probar la legitimidad del cliente que inicia la sesión con ese nombre de usuario. Por ese motivo, también es importante asegurar físicamente el servidor principal contra otros medios de acceso posibles.

Información de cabecera de BA de cliente original

opción de junctioncp: -b ignore

Esta opción indica a WebSEAL que ignore la cabecera de autentificación básica (BA) suministrada por el cliente. Informa a WebSEAL de que debe reenviar la cabecera, sin modificarla, al servidor de terceros. No se efectúa ningún inicio de sesión en el WebSEAL Server.

Este marco es el adecuado para un servidor principal que:

- Tenga soporte para la autentificación básica
- No esté configurado para usar la seguridad de Policy Director
- Deba mantener contraseñas suministradas por los clientes

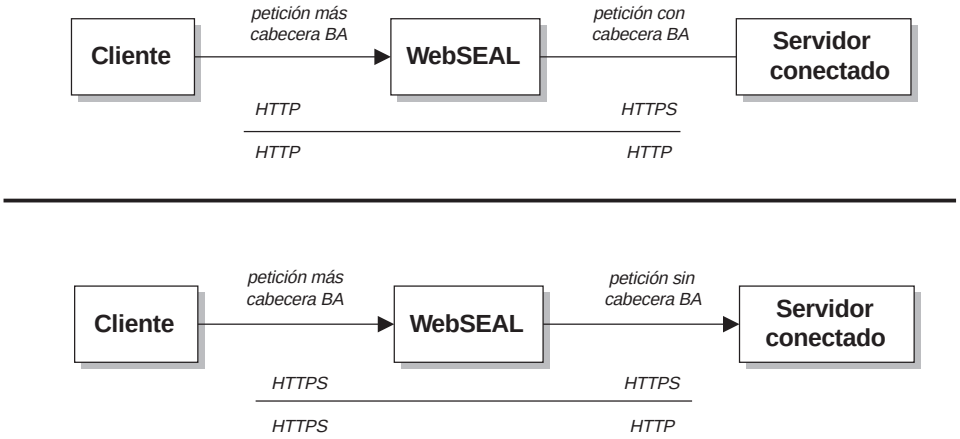
WebSEAL pasa directamente la petición del cliente original al servidor principal, sin interferencias.

El servidor principal devuelve una tentativa de autentificación básica al cliente. El cliente responde con la información del nombre de usuario y la contraseña, que WebSEAL Server pasa sin efectuar modificaciones.

No se trata de un verdadero mecanismo de conexión propia, sino de un iniciado de sesión directo con el servidor de terceros, que resulta transparente para WebSEAL.

PRECAUCIÓN:
Esta opción no funciona cuando el cliente se ha autentificado ante WebSEAL utilizando (la autentificación básica de) SSL. En este caso, la cabecera de autentificación básica se suprime como en (-b filter) antes de su envío a través de una conexión (junction) potencialmente insegura.

Si el servidor principal utiliza la autentificación básica, devolverá una tentativa al cliente. Pero la información de autentificación básica que devolverá el cliente volverá a borrarse. La petición no llegará nunca al servidor principal.

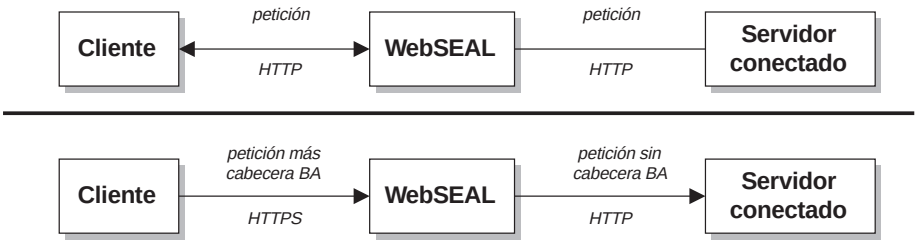


Sin información de autentificación

opción de junctioncp: -b filter

Esta opción indica a WebSEAL que elimine las cabeceras de autentificación básicas de las peticiones de clientes antes de reenviar las peticiones a los servidores principales. WebSEAL se convierte en el único proveedor de seguridad. Esta opción es adecuada cuando se sabe que el servidor principal no requiere autentificación básica.

Esta opción puede combinarse con la opción **-c** para insertar información de identidad del cliente de Policy Director en las cabeceras HTTP. Consulte el apartado “Inserción de información de la identidad del cliente (opción -c)” en la página 203.



Nombres de usuarios y contraseñas procedentes de GSO

opción de junctioncp: -b gso

Esta opción indica a WebSEAL que suministre al servidor principal información de autentificación (nombre de usuario y contraseña) procedente de GSO. Esto es adecuado cuando se desea tener seguridad tanto en WebSEAL como en los servidores principales. Las aplicaciones de servidores principales también requieren nombres de usuarios y contraseñas distintos que no se encuentran en el registro de WebSEAL.

En el apartado “Integración de la conexión propia de WebSEAL y GSO” en la página 213 se describe en detalle este mecanismo.

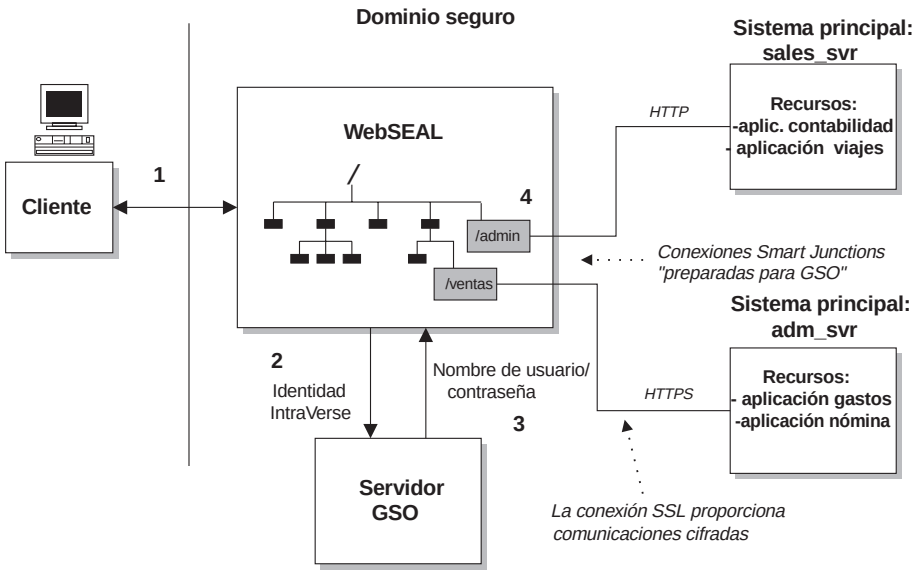
Integración de la conexión propia de WebSEAL y GSO

Policy Director tiene soporte para una solución de conexión propia más flexible gracias a la integración con IBM Global Sign-On (GSO). IBM Global Sign-On es un componente de la tecnología SecureWay de IBM. La combinación de WebSEAL y GSO proporciona una completa solución de única conexión para la Web que proporciona las ventajas adicionales que representan los datos cifrados, una alta disponibilidad y la escalabilidad.

La figura que sigue ilustra la integración de WebSEAL y GSO para recuperar nombres de usuarios y contraseñas para recursos de aplicaciones principales.

1. El cliente se autentifica ante WebSEAL con una petición de acceso a un recurso de aplicación de un servidor principal. Se obtiene una identidad de Policy Director.

   Nota: El proceso de conexión propia es independiente del método de autentificación inicial.
2. WebSEAL pasa la identidad de Policy Director a GSO.
3. GSO devuelve un nombre de usuario y la contraseña adecuados para el usuario y el recurso de aplicación solicitado.
4. WebSEAL inserta la información de nombre de usuario y contraseña en la cabecera de autentificación básica HTTP de la petición. WebSEAL envía la petición al servidor principal a través de la conexión Smart Junction.



Obtención de información de autentificación procedente de GSO

El siguiente ejemplo explica la forma en que GSO proporciona información de autentificación a WebSEAL. Cuando el usuario Miguel desea ejecutar el recurso de aplicación viajes-apl, WebSEAL pide a GSO información para la autentificación de Miguel.

GSO mantiene una base de datos completa con información sobre autentificaciones en forma de correlaciones de recursos con información de autentificación. La

correlación de recursos de aplicación con el nombre de usuario y la contraseña se denomina *Credenciales de recursos GSO*. Sólo pueden crearse Credenciales de recursos GSO para usuarios registrados.

GSO contiene una credencial de recurso específica para Miguel que correlaciona el recurso "viajes-apl" con una combinación de nombre de usuario y contraseña específica.

La siguiente tabla ilustra la estructura de la base de datos de recursos GSO.

Miguel	**Pablo**
recurso: viajes-apl nombre de usuario=miki contraseña=123 recurso: nómina-apl nombre de usuario=tola contraseña=456	recurso: viajes-apl nombre de usuario=vidal contraseña=abc recurso: nómina-apl nombre de usuario=camps contraseña=xyz

En este ejemplo, GSO devuelve a WebSEAL el nombre de usuario `miki` y la contraseña 123. WebSEAL utiliza esta información cuando crea la cabecera de autentificación básica HTTP en la petición que se envía a través de la conexión Smart Junction.

Configuración de una conexión Smart Junction habilitada para GSO

Configure soporte de WebSEAL para GSO en la conexión Smart Junction entre WebSEAL y un servidor principal de aplicaciones.

Para crear una conexión Smart Junction que habilite GSO, utilice el mandato **junctioncp create** con la opción **-b gso**. El siguiente ejemplo ilustra la sintaxis del mandato create:

```
create -t tcp -h nombre-sistema-principal -b gso -T
recurso  punto-conexión-Smart-Junction
```

La siguiente tabla indica las opciones para crear conexiones Smart Junction de GSO:

Opciones	**Descripción**
-b gso	Especifica que GSO debe proporcionar información de autentificación para todas las peticiones que atraviesen esta conexión (junction).
-T *recurso*	Especifica el nombre del recurso de aplicación. El nombre del recurso que se utilice como argumento para esta opción debe coincidir exactamente con el nombre del recurso listado en la base de datos de GSO. Necesario para conexiones Smart Junction de GSO.

Como se explica en el apartado "Creación de conexiones Smart Junction SSL seguras" en la página 204, puede conseguir que una conexión (junction) utilizada en una solución de WebSEAL y GSO sea segura a través de SSL. Asegúrela aplicando la opción **-t ssl** cuando cree la conexión Smart Junction.

Utilice siempre conexiones Smart Junction SSL con GSO para asegurar el cifrado de las Credenciales de recursos GSO y de todos los datos.

Ejemplos de conexiones Smart Junction habilitadas para GSO:

Conecte (junction) el recurso de aplicación “viajes-apl” del sistema principal “sales_svr” al punto de conexión Smart Junction “/sales”:

```
create -t tcp -b gso -T
viajes-apl -h sales_svr /sales
```

Conecte (junction) el recurso de aplicación “nómina-apl” del sistema principal “adm_svr” al punto de conexión Smart Junction “/admin” y asegure la conexión Smart Junction con SSL:

```
create -t ssl -b gso -T nómina-apl-h adm_svr /admin
```

Nota: En el ejemplo de arriba, la opción **-t ssl** indica la puerta por omisión 443.

Utilización de conexiones Smart Junction

Cada uno de los servidores principales debe conectarse a un punto de conexión Smart Junction (de montaje). A medida que la demanda de contenidos y recursos adicionales crece, podrá añadir más servidores utilizando conexiones Smart Junction.

Los apartados indicados a continuación están relacionados con la utilización de conexiones Smart Junction:

- “Montaje de varios servidores en la misma conexión Smart Junction”.
- “Filtrado de URL a través de servidores conectados con Smart Junction”.
- “Control del proceso de CGI (permiso x)” en la página 216

Montaje de varios servidores en la misma conexión Smart Junction

Se pueden montar varios servidores reproducidos en un mismo punto de conexión Smart Junction. Se pueden montar tantos servidores como se desee en un mismo punto.

Todos los servidores montados en un punto de conexión Smart Junction deben ser réplicas (espacios reflejados de la Web) y deben utilizar el mismo protocolo — HTTP o HTTPS. No monte servidores distintos en un mismo punto de conexión Smart Junction.

Desde el espacio de la Web del servidor primario de Policy Director, acceda a páginas que pertenezcan a los servidores conectados (junction). Debe poder acceder a estas páginas (sujeto a los permisos correspondientes, evidentemente) y las páginas deben parecer coherentes. Si ocasionalmente no puede encontrar una página o la página cambia, es que Policy Director no ha reproducido correctamente la página.

Asegúrese de que el documento existe y de que es idéntico en el árbol de documentos de los dos servidores reproducidos.

Filtrado de URL a través de servidores conectados con Smart Junction

Tan solo se filtran los documentos de tipo mime de “texto” o “html” procedentes de servidores conectados con Smart Junction.

Existen dos conjuntos de URL que WebSEAL puede cambiar: los absolutos y los relativos al sistema principal.

URL relativos al sistema principal

Un URL relativo al sistema principal indica una posición de URI en relación con el root del documento del servidor conectado con Smart Junction, por ejemplo:

```
/dir/file.html
```

Cambie estos URL para que reflejen el punto de conexión Smart Junction del servidor conectado con Smart Junction. Por ejemplo:

```
/jct/dir/file.html
```

URL absolutos

Un URL absoluto indica una posición de indicador de recurso universal (Universal Resource Indicator, URI) en relación con un nombre de SISTEMA PRINCIPAL o dirección IP y una puerta de red. Por ejemplo:

```
http://nombreservidor[:puerta]/archivo.html
```

O:

```
https://nombreservidor[:puerta]/archivo.html
```

Estos URL pueden cambiarse siguiendo estas normas:

1. Cuando el URL es HTTP y el sistema principal o la puerta coincide con un servidor TCP conectado con Smart Junction, el URL cambia para reflejar el punto de conexión Smart Junction. Por ejemplo:

   ```
   /jct/...
   ```

2. Cuando el URL es HTTPS y el sistema principal o la puerta coincide con un servidor SSL conectado con Smart Junction, el URL cambia para reflejar el punto de conexión Smart Junction. Por ejemplo:

   ```
   jct...
   ```

3. Sólo se filtran los URL para TAG y pares de atributos que estén definidos en el archivo de configuración iv.conf.
4. Filtre siempre los códigos META para peticiones de renovación. Por ejemplo:

   ```
   META HTTP-EQUIV="Refresh"
   CONTENT="5;URL=http://server/url"
   ```

5. Si un código BASE contiene un atributo HREF, el código se eliminará de la respuesta del cliente.

La sección [url-filter] del archivo de configuración iv.conf contiene parámetros para filtrar URL a través de servidores conectados con Smart Junction.

La sección [url-filter] contiene una lista de códigos HTML. El WebSEAL Server filtra o cambia estos códigos para ajustar los URL absolutos que se obtienen a través de un servidor conectado con Smart Junction-

Por omisión, Policy Director configura todos los códigos HTML utilizados frecuentemente. Es posible que el administrador tenga que añadir más códigos HTML que contengan URL.

Control del proceso de CGI (permiso x)

El permiso de ejecutar (x) de Policy Director no tiene significado a través de las conexiones Smart Junction. No se puede controlar el proceso de un script CGI con el permiso x. WebSEAL no tiene medios para determinar con precisión si un objeto solicitado perteneciente a un servidor principal es un archivo de un programa CGI

o un objeto normal de HTTP. El acceso a objeto, que incluye programas CGI, a través de conexiones Smart Junction siempre está controlado mediante la utilización del permiso de lectura (r).

Utilización de query_contents con servidores de terceros

Se pueden proteger los recursos del espacio de la Web de aplicaciones de terceros utilizando el servicio de seguridad de Policy Director. Cuando desee realizar esta operación, debe proporcionar a WebSEAL información sobre el contenido del espacio de la Web de terceros.

Un programa CGI llamado **query_contents** proporciona esta información. El programa **query_contents** busca el contenido del espacio de la Web y facilita esa información de inventario a Management Console en WebSEAL. El programa está incluido en la instalación de WebSEAL, pero deberá instalarlo manualmente en el servidor de terceros. Hay distintos tipos de archivos de programa distintos, dependiendo de si el servidor de terceros corresponde a la plataforma UNIX o a Windows.

El gestor del Espacio de objetos de Management Console puede ejecutar automáticamente **query_contents**. Se ejecuta cuando la porción del espacio de objetos protegidos, que representa la conexión (junction), se expande en el panel de gestión de Espacio de objetos. Cuando Management Console conoce el contenido del espacio de aplicaciones de terceros, se puede visualizar esta información y aplicar plantillas de políticas a los objetos adecuados.

Instalación de query_contents

Para instalar **query_contents** es necesario copiar uno o dos archivos de Policy Director Server en el servidor de terceros y editar un archivo de configuración.

El siguiente directorio de Policy Director contiene una plantilla del programa:

UNIX: *directorio-root*/www/lib/query_contents

Windows: *directorio-root*\www\lib\query_contents

El directorio contiene:

Archivo	Descripción
query_contents.exe	Programa principal ejecutable para sistemas Win32. Puede instalarse en el directorio cgi-bin del servidor Web de terceros.
query_contents.sh	Programa principal ejecutable para sistemas UNIX. Puede instalarse en el directorio cgi-bin del servidor Web de terceros.
query_contents.c	Código fuente. El fuente se proporciona por si es necesario modificar el comportamiento de **query_contents**. En la mayoría de los casos, no es necesario.
query_contents.html	Archivo de ayuda en formato HTML.
query_contents.cfg	Archivo de configuración de ejemplo que identifica el root de los documentos para el servidor Web.

Instalación de query_contents en servidores UNIX de terceros

Localice el script del shell llamado query_contents.sh en el directorio:

UNIX: *dir-instal*/www/lib/query_contents

Para instalar el programa de utilidad **query_contents** en servidores UNIX de terceros:

1. Copie query_contents.sh en un directorio /cgi-bin que funcione del servidor Web de terceros.
2. Suprima la extensión .sh.
3. Establezca el bit de "ejecutar" de UNIX para el usuario propietario del servidor Web.

Instalación de query_contents en servidores Win32 de terceros

Localice el programa ejecutable llamado query_contents.exe y el archivo de configuración llamado query_contents.cfg en el directorio:

Windows: *dir-instal*\www\lib\query_contents

Para instalar el programa de utilidad **query_contents** en servidores Win32 de terceros:

1. Asegúrese de que el servidor Web de terceros tiene un directorio CGI configurado correctamente.
2. Asegúrese de que hay un documento válido en el root de documentos del servidor Web de terceros.
3. Copie query_contents.exe en el directorio CGI del servidor Web de terceros.
4. Copie query_contents.cfg en el directorio de Windows.

   La siguiente tabla indica los valores por omisión de este directorio.

Sistema operativo	Directorio de Windows
Windows 95	c:\windows
Windows NT 3.5x	c:\winnt35
Windows NT 4.x	c:\winnt

5. Edite el archivo query_contents.cfg para especificar correctamente el directorio root de documentos del servidor Web de terceros.

   El archivo contiene actualmente las entradas de ejemplo de los servidores Microsoft Internet Information Server™ y Netscape® FastTrack. Las líneas de este archivo que empiezan por un punto y coma (;) son comentarios y el programa **query_contents** las ignora.

Prueba de la configuración

Para probar la configuración:

1. En el servidor Win32, vaya al directorio que contiene el programa **query_contents**.
2. Desde un indicador del DOS del servidor Win32, ejecute el programa:

   ```
   query_contents dirlist=/
   ```

   Verá una salida parecida a la siguiente:

```
100
index.html
cgi-bin//
pics//
```

El número 100 es un estado de retorno que indica una ejecución correcta. Es muy importante ver como mínimo el número 100 como primer (y quizá único) valor.

La aparición de un código de error en vez del 100 indica que el archivo de configuración no está en el lugar correcto o no contiene una entrada correcta de root de documentos. Compruebe la configuración del archivo query_contents.cfg y asegúrese de que el root de documentos existe.

3. En un navegador, entre el siguiente URL:

   `http: //`*`nombre-máquina-Win32`* `/cgi-bin/query_contents.exe?dirlist=/`

   Este mandato debería devolver el mismo resultado que el paso anterior. Si no devuelve este resultado, la configuración de la CGI del servidor Web no será correcta. Consulte la documentación del servidor para corregir el problema.

Configuración de una conexión Smart Junction para encontrar query_contents

Puede definir el URL para el script **query_contents**. Policy Director buscará **query_contents** en /cgi_bin/. Si este directorio es distinto o se ha cambiado el nombre del archivo **query_contents**, utilice esta opción para indicar a WebSEAL el nuevo URL del archivo.

Si crea la conexión Smart Junction para un servidor Win32 de terceros, utilice el mandato **junctioncp** con la opción **-q**:

```
junctioncp> create -t tcp -h nombre-sistema-principal -q
/cgi-bin/query_contents.exe /jct_mount_point
```

Si desea ver todas opciones del mandato **junctioncp**, consulte el apartado “Creación de una nueva conexión Smart Junction para un servidor inicial” en la página 198.

Ejecución de query_contents

Utilice **query_contents** para visualizar el contenido del directorio incluido en una petición de URL. Por ejemplo, para obtener el contenido del directorio root del espacio de la Web de un servidor, el navegador ejecuta **query_contents** en un URL como, por ejemplo:

```
http://servidor-de-terceros/cgi-bin/query_contents?dirlist=/
```

El script de **query_contents** realiza las siguientes operaciones:

1. Lee $SERVER_SOFTWARE, una variable estándar de entorno de CGI, para determinar el tipo de servidor.

   Policy Director coloca la variable $DOCROOTDIR en una ubicación típical del root de documentos, según el tipo de servidor Web.

2. Lee la variable de entorno $QUERY_STRING del URL solicitado para obtener la operación solicitada y la vía de acceso del objeto.

   La variable $OPERATION almacena el valor de la operación y $OBJPATH almacena la vía de acceso de la opción. En el ejemplo, $OPERATION es dirlist y $OBJPATH es “ / ”.

3. Realiza un listado de directorios (ls) de la vía de acceso del objeto y coloca los resultados en salida estándar para que la utilice el servidor de Policy Director. Las entradas que indican subdirectorios llevan una doble barra inclinada (//) a continuación.

   Una salida normal sería parecida a esta:

   ```
   100
   index.html
   cgi-bin//
   pics//
   ```

   El número 100 es un estado de retorno que indica una ejecución correcta.

Personalización de query_contents

Para personalizar **query_contents** para su servidor, quizá necesite cambiar la situación del directorio root de documentos.

Si devuelve un estado de error (un número distinto de 100) y no lista ningún archivo, examine el script. Si lo considera necesario, cambie la variable $DOCROOTDIR para que se ajuste a la configuración del servidor.

Si especifica correctamente el directorio root de documentos y el script sigue sin ejecutarse correctamente, es posible que la especificación de la ubicación de cgi-bin sea incorrecta. Examine la variable $FULLOBJPATH y cambie el valor que tiene asignado para que refleje la ubicación correcta de cgi-bin.

Funcionalidad adicional

El código fuente del programa **query_contents** (query_contents.c) se distribuye con Policy Director.

Puede añadir otras funciones a este programa para dar soporte a características especiales de algunos servidores Web de terceros. Estas características incluyen:

1. Correlación de directorios—cuando un subdirectorio que no está por debajo del root de documentos se correlaciona con el espacio de la Web.
2. Generación de un espacio de la Web que no esté basado en el sistema de archivos.

   Podría tratarse de un servidor Web de una base de datos de sistema principal.

Capítulo 16. WebSEAL: integración de aplicaciones

WebSEAL tiene soporte para la integración de aplicaciones de terceros a través de variables de entorno y la posibilidad de utilización de URL dinámicos. WebSEAL amplía la gama de variables de entorno y cabeceras HTTP para permitir a las aplicaciones de terceros realizar operaciones basadas en la identidad del cliente. Además, WebSEAL puede proporcionar control de accesos a URL dinámicos como, por ejemplo, los que contienen texto de consulta.

Este capítulo incluye los siguientes temas:

Soporte para programación de CGI

Para dar soporte a la programación de CGI, WebSEAL añade tres tres variables de entorno al conjunto estándar de variables de entorno de CGI. Las aplicaciones CGI puede utilizar estas variables de entorno que se ejecutan tanto en el WebSEAL Server local como en un servidor principal conectado con Smart Junction. Las variables proporcionan a la aplicación CGI información específica de Policy Director sobre usuarios, grupos y credenciales.

En un WebSEAL Server local, la información de credencial de Policy Director sobre el cliente que efectúa la petición produce directamente dichas variables de entorno.

Las variables de entorno que utiliza una aplicación CGI que se ejecuta en un servidor de terceros conectado con Smart Junction las produce las información de cabecera HTTP. WebSEAL pasa la información de cabecera HTTP al servidor. Es necesario utilizar la opción**-c** de **junctioncp** para crear una *junction* (conexión). La conexión Smart Junction inserta entonces la información de cabecera específica de Policy Director en las peticiones HTTP destinadas a un servidor principal.

Consulte el apartado "Inserción de información de la identidad del cliente (opción -c)" en la página 203.

Variables de entorno adicionales específicas de Policy Director

A continuación se indican los formatos de las variables de entorno de CGI específicas de Policy Director:

Formato de variable de entorno CGI	Descripción
HTTP_IV_USER	Nombre de la cuenta de usuario Policy Director del solicitante.
HTTP_IV_GROUPS	Grupos de Policy Director a los que pertenece el solicitante. Se especifica como una lista separada por comas de nombres de grupo entre comillas dobles.

HTTP_IV_CREDS	Estructura de datos opacos codificados que representa una credencial de Policy Director. Facilita credenciales a servidores remotos para que aplicaciones de la gama media puedan utilizar la API de autorizaciones para llamar a Authorization Service. Consulte el manual *Policy Director Programmer's Guide and Reference.*

La variable REMOTE_USER en WebSEAL Server local

En un entorno de servidor local controlado por WebSEAL, el valor de la variable HTTP_IV_USER se facilita como valor de la variable estándar REMOTE_USER. Tenga en cuenta que la variable REMOTE_USER también puede encontrarse en el entorno de una aplicación CGI que se ejecute en un servidor principal conectado (junction). No obstante, en esa situación, WebSEAL no controlará su valor.

Formato de variable de entorno CGI	**Descripción**
REMOTE_USER	Contiene el mismo valor que el campo HTTP_IV_USER.

Soporte de aplicaciones del área del servidor principal

WebSEAL también proporciona soporte para código ejecutable que se ejecute como componente incorporado a un servidor Web principal. Este código ejecutable del área del servidor incluye, por ejemplo:

- servlets Java
- Cartuchos para Oracle Web Listener
- Conexiones (plugin) del área del servidor

Puede crear una conexión Smart Junction con un servidor principal utilizando la opción **-c** del programa de utilidad **junctioncp**. A continuación, WebSEAL inserta información específica de Policy Director de identidad y pertenencia a grupos del cliente en las cabeceras de las peticiones HTTP destinadas al servidor.

Consulte el apartado "Inserción de información de la identidad del cliente (opción -c)" en la página 203.

Las cabeceras HTTP específicas de Policy Director permiten a las aplicaciones de servidores de terceros conectados con Smart Junction realizar acciones específicas sobre la identidad Policy Director del cliente.

WebSEAL proporciona la siguiente información de cabecera HTTP específica de Policy Director:

cabeceras HTTP específicas de Policy Director	**Descripción**
iv-user	El nombre del cliente. Por omisión es "No autentificado" cuando el cliente no está autentificado (es desconocido).
iv-groups	Una lista grupos a los que pertenece el cliente. Es una lista separada por comas de nombres de grupos entre comillas dobles.
iv-creds	Estructura de datos opacos codificados que representa una credencial de Policy Director. Facilita credenciales a servidores remotos para que aplicaciones de la gama media puedan utilizar la API de autorizaciones para llamar a Authorization Service. Consulte el manual *Policy Director Programmer's Guide and Reference*.

Estas entradas de HTTP están disponibles para aplicaciones CGI como variables de entorno HTTP_IV_USER, HTTP_IV_GROUP y HTTP_IV_CREDS. Para otros productos de infraestructura de aplicaciones que no son de CGI, consulte la documentación asociada al producto donde encontrará las instrucciones pertinentes para la extracción de cabeceras de peticiones HTTP.

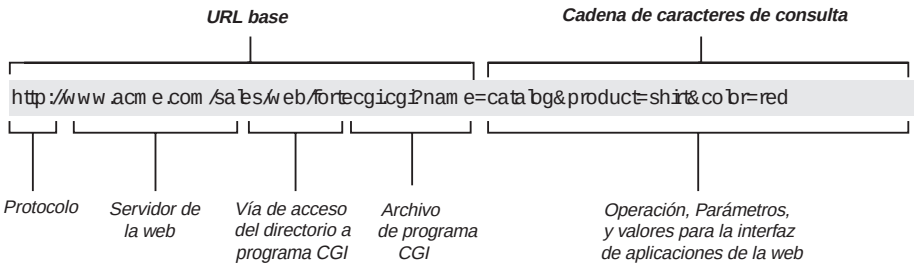
Posibilidad de control de accesos para URL dinámicos

El entorno actual de la Web proporciona a los usuario un acceso inmediato que permite intercambiar información con rapidez. Muchas aplicaciones de la Web generan rápidamente Uniform Resource Locators (URL) en respuesta a cada petición de usuario. Es posible que estos URL dinámicos sólo duren un corto periodo de tiempo. A pesar de su naturaleza temporal, sigue siendo proteger los URL dinámicos contra utilizaciones o accesos no deseados.

Qué son los URL dinámicos

Algunas herramientas sofisticadas de aplicaciones de la Web utilizan navegadores estándar de la Web para comunicarse con servidores de aplicaciones a través de la interfaz CGI de un servidor Web.

Todas estas herramientas utilizan URL dinámicos y elementos ocultos para comunicar la operación solicitada (con su valor de parámetro) al servidor de aplicaciones. Un URL dinámico aumenta la dirección estándar del URL con información sobre la operación específica y sus valores de parámetro. La porción de la operación de consulta del URL proporciona operaciones, parámetros y valores a la interfaz de aplicación de la Web.



Correlación objetos del espacio de nombres de ACL con URL dinámicos

WebSEAL utiliza el modelo de espacio de nombres de objetos protegidos y las plantillas de políticas (ACL) para asegurar URL generados de forma dinámica, como los URL generados por peticiones de la base de datos. Cada petición a WebSEAL se resuelve en un objeto específico del espacio de nombres como primer paso del proceso de autorización. Cuando se aplica una ACL al objeto del espacio de nombres, ésta indica la protección necesaria para cualquier URL correlacionado con dicho objeto.

Como los URL dinámicos sólo existen temporalmente, no es posible tener entradas para ellos en una base de datos de políticas de autorización preconfigurada. WebSEAL resuelve este problema proporcionando un mecanismo que correlaciona muchos URL con un solo objeto estático protegido.

Un archivo de texto contiene las correlaciones de patrones de objetos con el espacio de nombres de objetos.

UNIX: /opt/intraverse/www/lib/dynurl.conf

Windows: C:\Archivos de programa\IBM\Policy Director\www\lib\dynurl.conf

Edite este archivo si desea cambiar las correlaciones. Es necesario crear este archivo, no existe por omisión. Las entradas del archivo tiene el siguiente formato:

objeto patrón

WebSEAL utiliza un subconjunto de patrones de shell de UNIX (que incluye comodines) que define el conjunto de parámetros que constituye un objeto del espacio de nombres. WebSEAL correlaciona con dicho objeto todos los URL que coinciden con estos parámetros. WebSEAL tiene soporte para los siguientes caracteres de coincidencia con un patrón del shell de UNIX:

Carácter	Descripción
\	El carácter que sigue a la barra inclinada forma parte de una secuencia especial. Es, por ejemplo, es carácter del TABULADOR.
?	Comodín que coincide con un solo carácter. Por ejemplo, la cadena de caracteres abcde coincide con la expresión ab?de.
*	Carácter que coincide con cero o más caracteres.
[ ]	Define un conjunto de caracteres del que puede coincidir cualquier carácter. Por ejemplo, la cadena de caracteres abcde coincide con la expresión regular ab[cty]de.
^	Indica una negación. Por ejemplo, la expresión ^[ab] lo compara todo menos los caracteres 'a' o 'b'.

El siguiente ejemplo indica el formato de un URL dinámico que efectúa la búsqueda de un saldo de crédito.

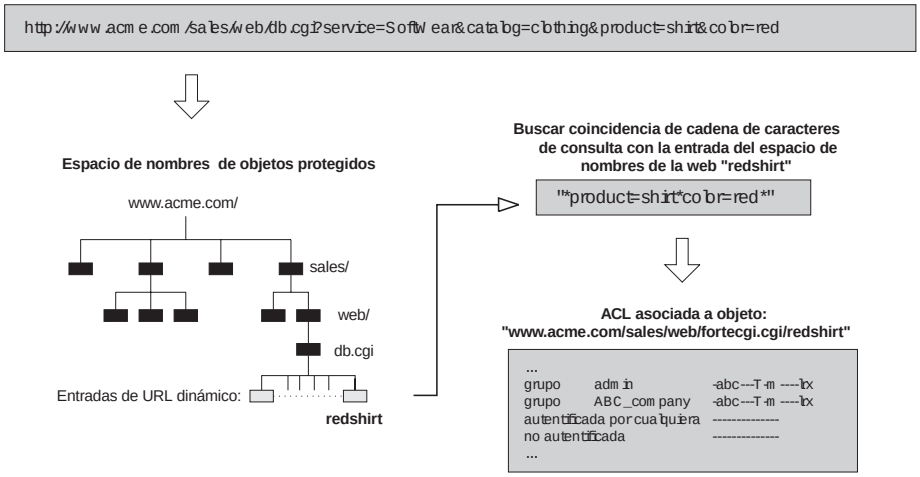
http: //*nombre-servidor*/banco-local/owa/acct.bal?acc=*número-cuenta*

El objeto del espacio de nombres espacio de nombres que representa este URL dinámico se visualizará como sigue:

http: //<nombre-servidor>/banco-local/owa/acct.bal?acc=*

Examinando detenidamente el URL dinámico de este ejemplo puede verse que describe un número de cuenta específico. El objeto del espacio de nombres para saldos de cuentas de banco-local, indica que los permisos de la ACL se aplican a cualquier cuenta. Se aplican a cualquier cuenta porque la última porción de la entrada (acc=*) utiliza el carácter comodín asterisco que coincide con todos los caracteres.

Esta figura ilustra un ejemplo completo de un URL dinámico específico correlacionado con un objeto del espacio de nombres protegido. Este ejemplo no utiliza ningún comodín.



Actualización de WebSEAL para URL dinámicos

Utilice el programa de utilidad **dynurlcp** para actualizar el espacio de nombres de objetos protegidos de WebSEAL con entradas que se efectúan en el archivo de configuración dynurl.conf. Debe iniciar la sesión con el dominio seguro utilizando dce_login.

Para utilizar el programa de utilidad **dynurlcp** a fin de actualizar el espacio de nombres de objetos protegidos de WebSEAL:

1. Cree, edite o elimine una entrada de URL dinámico en el archivo de configuración dynurl.conf.
2. Después de realizar las modificaciones, utilice el programa de utilidad **dynurlcp** para actualizar el servidor.

   ```
   dynurlcp -e /.:/subsys/intraverse/secmgr/server/ host update
   ```

Resolución de URL dinámicos en el espacio de nombres

La resolución de un URL dinámico para un objeto del espacio de nombres depende del orden de las entradas en el archivo de configuración dynurl.conf.

Cuando se intenta correlacionar un URL dinámico con una entrada del espacio de nombres, se explora la lista de correlaciones del archivo de configuración dynurl.conf. El archivo se examina del principio al fin hasta que se encuentra el primen patrón coincidente.

Una vez encontrada la primera coincidencia, WebSEAL utiliza la entrada del espacio de nombres correspondiente para la siguiente autorización. Cuando no se encuentra ninguna coincidencia, WebSEAL usa el URL propiamente dicho menos la porción `http://servidor` de la vía de acceso.

Conserve las correlaciones que correspondan a las ACL más restrictivas al principio de la lista. Por ejemplo, el procedimiento de venta de libros (de una aplicación de pedidos de venta) está limitado únicamente a los miembros de un club literario. Sin embargo, todos los usuarios pueden acceder al resto de la aplicación de pedidos de venta. La correlación debería estar en el orden que se indica en esta tabla:

Entrada del espacio de nombres	Patrón de URL
/ows/sales/bksale	/ows/db-apps/owa/book.sales*

/ows/sales/general	/ows/db-apps/owa/*

Tenga en cuenta que si las entradas de correlación estuviesen en el orden inverso, todos los procedimientos del directorio /ows/db-apps/owa se correlacionarían con el objeto del espacio de nombres /ows/sales/general. Debido a esta resolución incorrecta del espacio de nombres, podrían producirse violaciones de la seguridad.

Métodos GET y POST de transmisión de datos

Cuando se correlaciona una expresión normal de un URL con una entrada del espacio de nombres, el formato del URL debe asumir el formato que se obtiene con el método GET. Para que este supuesto se produzca, no importa si se utiliza el método POST o el GET.

En el método GET de transmisión de datos, WebSEAL añade los *datos dinámicos* al URL. Un ejemplo de datos dinámicos sería los datos que se suministran en un formulario para un usuario.

En el método POST de transmisión de datos, WebSEAL incluye los datos dinámicos en el cuerpo de la petición.

Evaluación de ACL

Después de haber resuelto el URL dinámico en una entrada del espacio de nombres, se utiliza el modelo estándar de valores heredados de ACL de Policy Director. Este modelo determina si la petición debe procesarse o prohibirse (porque los privilegios son insuficientes).

Descripción de un URL dinámico: El Reino de los Viajes

El siguiente ejemplo explica cómo la intranet de una empresa puede asegurar URL generados por un Oracle Web Listener.

El servidor de URL dinámicos de la Web utilizado en este ejemplo es el Oracle Web Listener. Esta tecnología puede aplicarse del mismo modo a otros servidores de URL dinámicos de la Web.

La aplicación

El Reino de los Viajes es una empresa que ofrece a sus clientes un servicio de reservas de pasajes a través de Internet. Esta empresa tiene la intención de operar con dos aplicaciones de base de datos Oracle en su servidor Web—al que puede accederse desde dentro del cortafuego de la empresa y a través de Internet.

- **Sistema de reservas de pasajes**

  Los clientes autorizados puede efectuar reservas de forma remota y efectuar consultas sobre sus propias reservas. El personal del Reino de los Viajes también puede hacer reservas de clientes por teléfono, procesar cambios y realizar muchas otras transacciones. Como los clientes externos pagan los servicios con tarjetas de crédito, WebSEAL debe asegurar enormemente la transmisión de la información.

- **Gestor de administración**

  Como muchas otras empresas, El Reino de los Viajes mantiene una base de datos de administración que contiene información sobre sueldos, cargos y experiencia. Una fotografía de cada empleado de la empresa acompaña estos datos.

La interfaz

Un servidor Web Oracle puede configurarse para que proporcione acceso a los siguientes procedimientos de la base de datos:

/db-apps/owa/tr.browse	Permite a los usuarios consultar destinos, precios, etc., sobre viajes.
/db-apps/owa/tr.book	Se utiliza para hacer una reserva (personal de la agencia de viajes o clientes autentificados).
/db-apps/owa/tr.change	Se utiliza para revisar o cambiar las reservas actuales.
/db-apps/owa/admin.browse	Puede utilizarlo cualquier empleado de la empresa para ver información no restringida sobre el personal como, por ejemplo, número de extensión, dirección de correo electrónico y fotografía.
/db-apps/owa/admin.resume	Permite a un empleado de la empresa ver o cambiar su información resumida en la base de datos de administración.
/db-apps/owa/admin.update	Utilizado por el personal de administración para actualizar la información sobre el personal.

Estructura del espacio de la Web

Utilice un WebSEAL Server para proporcionar una interfaz segura con el espacio unificado de la Web del Reino de los Viajes.

Puede efectuar una conexión Smart Junction (/ows) con el servidor Web Oracle que ejecuta la aplicación de reservas de pasajes y la aplicación de administración.

La política de seguridad

Para proporcionar una seguridad adecuada a los recursos de la Web y seguir teniendo un sistema fácil de usar, la empresa ha definido los siguientes objetivos de seguridad:

- Los empleados de la agencia de viajes tiene un control completo sobre todas las reservas.
- Los usuarios autentificados puede efectuar y cambiar sus propias reservas, pero no pueden interferir con los datos de viajes de otros clientes autentificados.
- Los miembros del departamento de administración tienen un acceso completo a toda la información de administración.
- El personal del Reino de los Viajes que no pertenezca al departamento de administración puede cambiar su información resumida y ver información parcial del resto de empleados de la empresa.

Correlaciones de URL dinámicos con el espacio de nombres

Para conseguir los objetivos de política de seguridad, deben configurarse las correlaciones de URL dinámicos con entradas entradas del espacio de nombres de ACL. Recuerde que el orden de dichas correlaciones es una parte importante para conseguir los objetivos de seguridad.

Las correlaciones deben configurarse como se indica en esta tabla:

Entrada del espacio de nombres	Patrón de URL
/ows/tr/browse	/ows/db-apps/owa/tr.browse\?dest=*&date=??/??/????

/ows/tr/auth	/ows/db-apps/owa/tr.book\?dest=*&depart=??/??/????&return=??/??/????
/ows/tr/auth	/ows/db-apps/owa/tr.change
/ows/admin/forall	/ows/db-apps/owa/admin.resume
/ows/admin/forall	/ows/db-apps/owa/admin.browse\?empid=[th]???
/ows/admin/auth	/ows/db-apps/owa/admin.update\?empid=????

Los clientes seguros

Los clientes se autentifican ante WebSEAL a través de un canal seguro y cifrado.

Los clientes que deseen utilizar la interfaz de la Web deberán, además, registrarse con el maestro de la Web del Reino de los Viajes para recibir una cuenta.

Estructura de cuentas y estructura de grupos

Cree los siguientes grupos en el sistema:

Personal	Empleados de la empresa El Reino de los Viajes.
PersonalRV	Agentes de viajes del Reino de los Viajes
PersAdmin	Miembros del departamento de administración. Tenga en cuenta que los empleados del departamento de administración también se encuentran en el grupo Personal.
Clientes	Clientes del Reino de los Viajes que desean efectuar sus reservas de pasajes a través de Internet.

Proporcione a cada usuario una cuenta en el dominio seguro para que el WebSEAL Server pueda identificarlos individualmente. WebSEAL pasa la identidad de los usuarios a los servidores Web Oracle y proporciona una solución de conexión propia para todos los recursos de la Web.

El control de accesos

La siguiente tabla lista los controles de acceso que resultan de la aplicación de la anterior información:

/ows/tr/browse	no autentificado	Tr
	autentificado por cualquiera	Tr
/ows/tr/auth	no autentificado	-
	autentificado por cualquiera	-
	grupo PersonalRV	Tr
	grupo Clientes	PTr
/ows/admin/forall	no autentificado	-
	autentificado por cualquiera	-
	grupo Personal	Tr
/ows/admin/auth	no autentificado	-
	autentificado por cualquiera	-
	grupo PersAdmin	Tr

Clientes y PersonalRV tienen los mismos privilegios sobre los objetos de reservas y mantenimiento de planes de viajes, con una excepción. La excepción consiste en que los clientes deben cifrar la información (permiso de privacidad) para tener más seguridad cuando transmitan *datos confidenciales* a través de Internet que es una red poco fiable. Los datos confidenciales serían, por ejemplo, la información de la tarjeta de crédito.

La conclusión

Este simple ejemplos describe los conceptos integrados en la utilización de un sistema que pueda:

- Asegurar información confidencial
- Autentificar usuarios
- Autorizar el acceso a información confidencial

Además, las identidades de los usuarios autentificados del sistema son conocidas por los servidores WebSEAL y Oracle de la Web. Las identidades se utilizan para proporcionar una solución de conexión propia auditable.

Capítulo 17. NetSEAL: visión general

NetSEAL es una solución de Virtual Private Network (VPN) para asegurar las comunicaciones entrantes TCP/IP. Como gestor de recursos, NetSEAL controla la posibilidad por parte de un usuario de conectarse con una aplicación específica TCP. NetSEAL realiza el control de accesos basándose en la puerta de destino y en la identidad del cliente. NetSEAL permite la integración de cualquier servidor de aplicaciones de la red con servicios de seguridad de Policy Director.

Este capítulo incluye los siguientes temas:

Presentación de NetSEAL

NetSEAL permite un acceso controlado a aplicaciones y servicios basados en TCP en un dominio seguro de Policy Director. Los clientes Windows tienen comunicaciones seguras con NetSEAL a través del cliente NetSEAT de Policy Director.

Las comunicaciones entre NetSEAT y NetSEAL pueden asegurarse utilizando un túnel (tunnel) SSL o un túnel GSS. En cada caso, el enlace seguro establecido entre un cliente NetSEAT y un servidor Policy Director se autentifica utilizando el nombre de usuario y la contraseña del cliente que efectúa la petición.

- Utilice un *canal SSL* para asegurar la comunicación entre NetSEAT y NetSEAL.
- Utilice *túneles GSS* o conexiones Smart Junction de NetSEAL para asegurar la comunicación de un servidor NetSEAL a un servidor NetSEAL. Los túneles GSS establecidos entre servidores Policy Director se autentifican siempre utilizando el usuario del servidor Policy Director que efectúa la conexión en nombre del cliente que efectúa la petición. A través del túnel GSS, los dos servidores se autentifican mutuamente; el segundo servidor siempre realiza el control de accesos sobre el cliente.

Las conexiones Smart Junction de NetSEAL establecen la dirección de avance de la comunicación a través de un servidor Policy Director y hasta otro servidor Policy Director o red. Utilice un túnel GSS para asegurar la comunicación a través de una conexión Smart Junction de NetSEAL.

El control de accesos de NetSEAL es flexible. Existe control hasta la puerta específica en la que la aplicación está a la escucha. Los recursos manipulados por la aplicación no sacan ninguna ventaja de un control de accesos estricto.

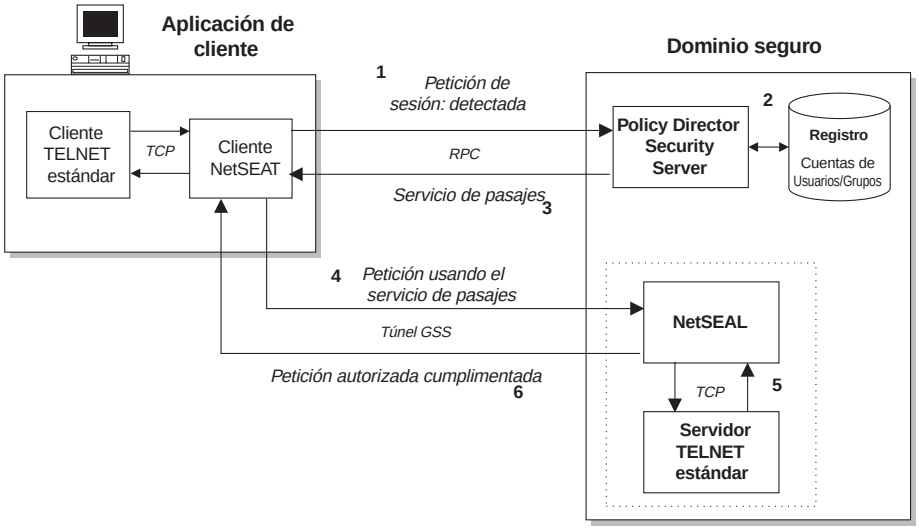
Este capítulo contiene varios ejemplos de red en los que se utiliza NetSEAL. En los diagramas, se utiliza la aplicación de inicio de sesión remoto de TELNET como ejemplo de aplicación TCP. En cada ejemplo, NetSEAL responde a una petición basada en:

- El origen de la petición
- Los permisos que afectan a los objetos (como, por ejemplo, las puertas de destino y las conexiones (junctions) de NetSEAL
- Los principales implicados en la conexión

Cliente NetSEAT con NetSEAL a través de un túnel GSS

Cuando NetSEAT se ha configurado para utilizar un túnel GSS, NetSEAT detecta la salida de la petición y, utilizando RPC, autentifica el cliente ante Policy Director Security Server. Además, se realiza una comprobación de seguridad para saber cuál es la puerta asociada a la aplicación solicitada.

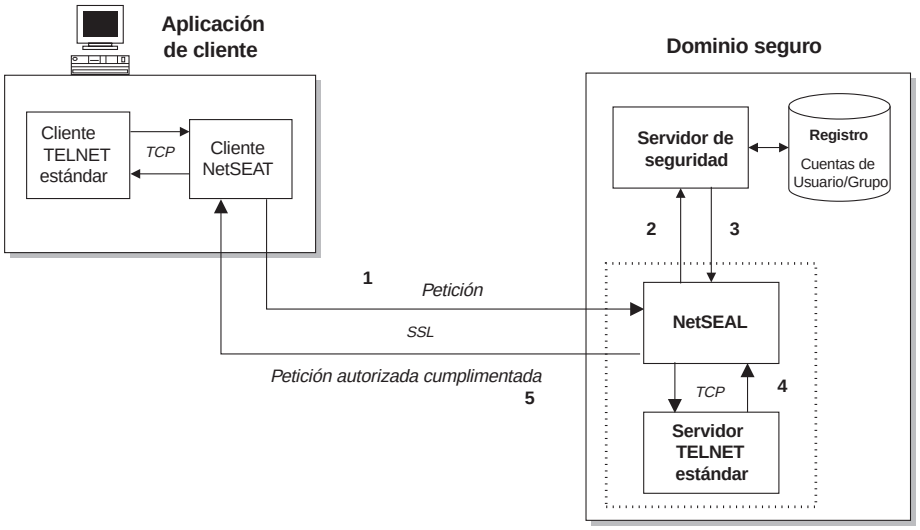
Si el proceso de autentificación y autorización resulta favorable, se establecerá un túnel (″tunnel″) GSS entre NetSEAT y NetSEAL Server. El acceso a la aplicación TCP solicitada desde NetSEAL se efectúa utilizando TCP.



Cliente NetSEAT con NetSEAL a través de SSL

Cuando se configura NetSEAT para que utilice SSL, la autentificación y la autorización las gestionan entre NetSEAL y los Policy Director Security Services. NetSEAL puede aceptar un nombre de usuario y una contraseña como identidad del cliente.

Si los procesos de autentificación y autorización son favorables, Policy Director procesará la petición. Utilice TCP para acceder a la aplicación TCP solicitada desde NetSEAL.

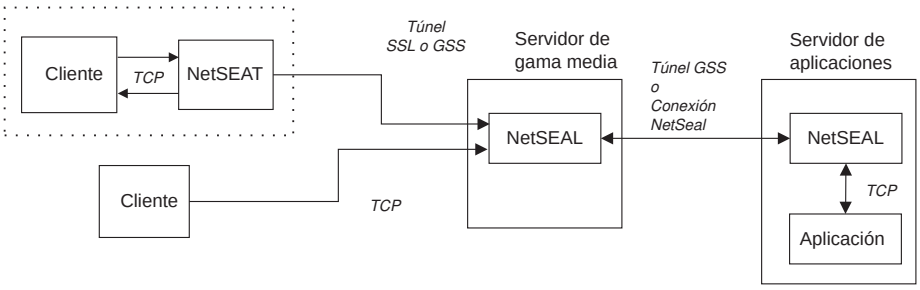


Segmentos de red de NetSEAL

La petición de conexión en una transacción de NetSEAL experimenta distintos niveles de protección a lo largo de su recorrido en la red. Como se explica en el apartado “Cliente NetSEAT con NetSEAL a través de SSL” en la página 232, el cliente NetSEAT tiene soporte para una conexión SSL o GSS con el servidor NetSEAL.

Nota: Debido a su diseño, la conectividad de NetSEAL Server con NetSEAL Server es *siempre* GSS. No utilice una conexión SSL entre dos servidores NetSEAL.

La trayectoria final desde NetSEAL hasta la puerta de la aplicación TCP local o remota se efectúa siempre mediante TCP.



La siguiente tabla resume el nivel de protección de cada segmento de conexión:

Segmento de conexión	Protección
Cliente NetSEAT con servidor NetSEAL	Túnel SSL o GSS
Cliente TCP con servidor NetSEAL	Ninguna
Servidor NetSEAL con servidor NetSEAL	Túnel GSS
Conexiones Smart Junction de NetSEAL	Túnel GSS
Servidor NetSEAL con puerta de aplicación TCP	Ninguna

NetSEAL sigue el mismo proceso de decisión de conexión para aplicaciones locales y remotas:

- ¿Está protegida la puerta solicitada (con una ACL)?
- Si se trata de una puerta protegida ¿tiene el usuario el permiso adecuado para tener acceso?
- Si se trata de una puerta no protegida, permitir la conexión saliente.

NetSEAL también separa la emisión de información entrante que requiere Security Manager y del proceso de conexión de salida. En otras palabras, Security Manager no necesita saber si el cliente NetSEAT detecta al petición de conexión local o remotamente.

Descripción de los servicios de cliente con NetSEAL

Los siguientes ejemplos describen los tipos de interacciones posibles entre un cliente y una aplicación TCP protegida por NetSEAL. Los clientes pueden ser tanto NetSEAT como no NetSEAT.

Los ejemplos son los siguientes:

- "Conexión tunelizada (″tunnel″) entrante con Policy Director Server".
- "Conexión tunelizada (″tunnel″) entrante con un sistema principal protegido" en la página 235.
- "Conexión TCP entrante con Policy Director Server" en la página 236.

Conexión tunelizada (″tunnel″) entrante con Policy Director Server

En este primer supuesto básico, se configura un cliente NetSEAT para detectar conexiones salientes destinadas a una aplicación del Policy Director Server. Cuando el cliente NetSEAT detecta la comunicación, se establece un túnel con NetSEAL en el Policy Director Server. La petición de este ejemplo destinada a la puerta 23 se envía a través de este túnel.

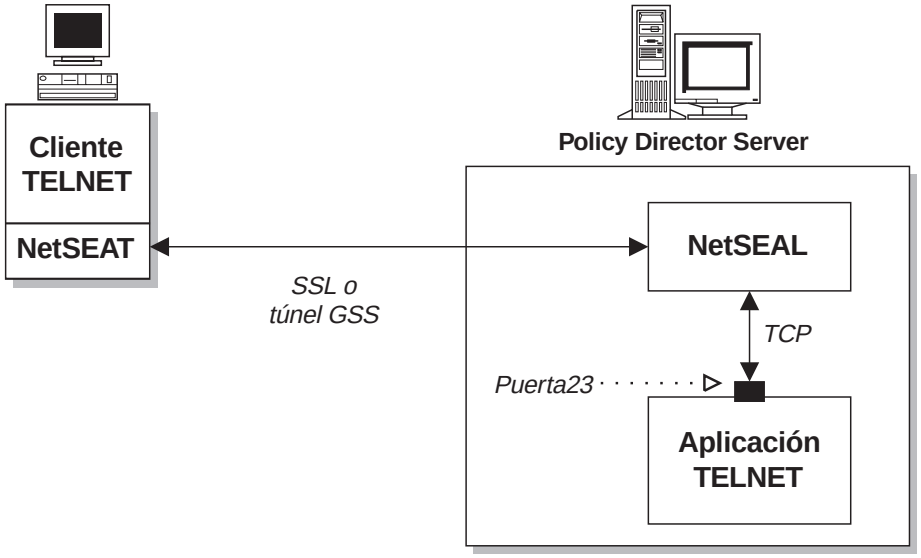
El proceso de autentificación es transparente para el usuario.

El NetSEAL Server completa la transacción como sigue:

1. Basándose en la ACL de la puerta ¿puede el usuario conectar con la puerta solicitada?

   Sí—Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.



Conexión tunelizada (″tunnel″) entrante con un sistema principal protegido

Este ejemplo presenta una aplicación que reside en un servidor remoto protegido. El servidor de aplicaciones puede ser un servidor Policy Director o un servidor de terceros. Policy Director utiliza siempre GSS para la comunicación entre dos NetSEAL Servers.

En este caso, NetSEAL puede proteger aplicaciones TCP que se ejecuten en plataformas no soportadas por Policy Director.

El NetSEAL Server completa la transacción como sigue:

1. ¿Puede conectar el usuario con la puerta solicitada del servidor de destino (basándose en la ACL)?

   Sí—Continuar.

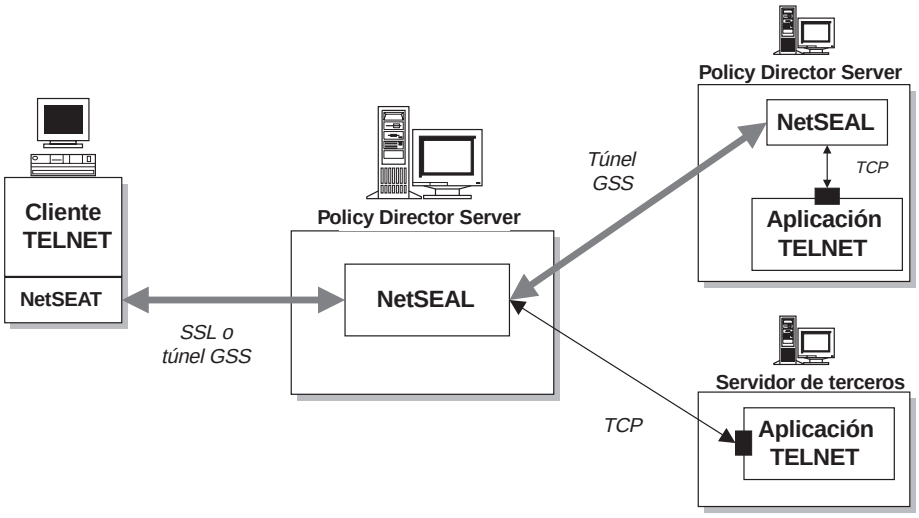
   No—Rechazar la petición de conexión.

2. ¿Es el destino un Policy Director Server?

   Si—Establecer un túnel seguro con el servidor. Establecer una conexión TCP con la puerta solicitada.

   No—Establecer una conexión TCP (insegura) con la puerta solicitada.

Un servidor de aplicaciones de terceros tiene siempre una conexión TCP desprotegida. Utilice una configuración de este tipo en un entorno de red fiable.



Conexión TCP entrante con Policy Director Server

Este ejemplo plantea la situación para un usuario de cliente TCP que no es NetSEAT. Policy Director reconoce los clientes de este tipo como no autentificados. Si la puerta solicitada no está protegida (no tiene ACL), Policy Director permitirá el acceso a dicha puerta. Si una ACL protege la puerta, Security Manager comprobará la ACL para saber si permite un acceso no autentificado.

Esa configuración protege el acceso directo a servicios de red. Un servicio de autorizaciones externo podría utilizar la dirección IP del cliente para determinar sus derechos de acceso.

El NetSEAL Server completa la transacción como sigue:

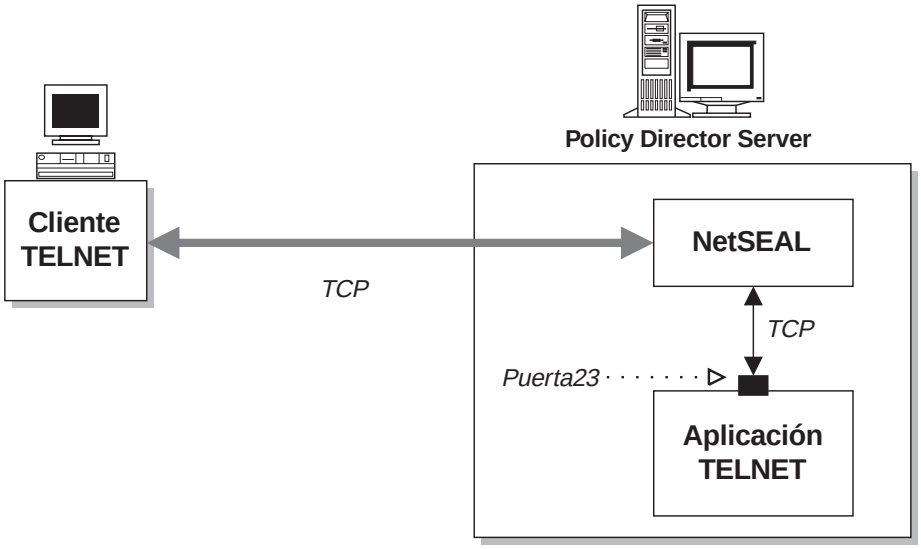
1. ¿Ha detectado Policy Director la petición (hay una ACL en la puerta)?

   Sí—Pasar la petición a Security Manager (secmgrd).

   No—Permitir la conexión entrante.
2. ¿Están permitidas las peticiones no autentificadas en la puerta?

   Sí—Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.



Descripción de servicios de NetSEAL a NetSEAL

Los siguientes ejemplos describen los tipos de interacciones posibles entre dos servidores. En estos ejemplos, las conexiones las inicia el primer NetSEAL Server (con un cliente local) vez de que se inicien desde un cliente NetSEAT remoto.

En estos ejemplos, las conexiones las inicia el primer NetSEAL Server (con un cliente local) vez de que se inicien desde un cliente NetSEAT remoto. Este cliente local podría operar desde TELNET o la consola del servidor para un servidor remoto. Un NetSEAL Server principal puede proteger la aplicación TCP.

Los ejemplos son los siguientes:

- "Conexión de salida con Policy Director Server".
- "Conexión de salida con sistema principal protegido" en la página 238.

Conexión de salida con Policy Director Server

Utilice un túnel GSS para efectuar una conexión entre dos Policy Director NetSEAL Servers. El primer NetSEAL Server (con un cliente local) inicia la conexión en vez de que se inicie desde un cliente NetSEAT remoto. Policy Director puede permitir o denegar una conexión y proteger cualquier comunicación permitida.

El Policy Director Server completa la transacción como sigue:

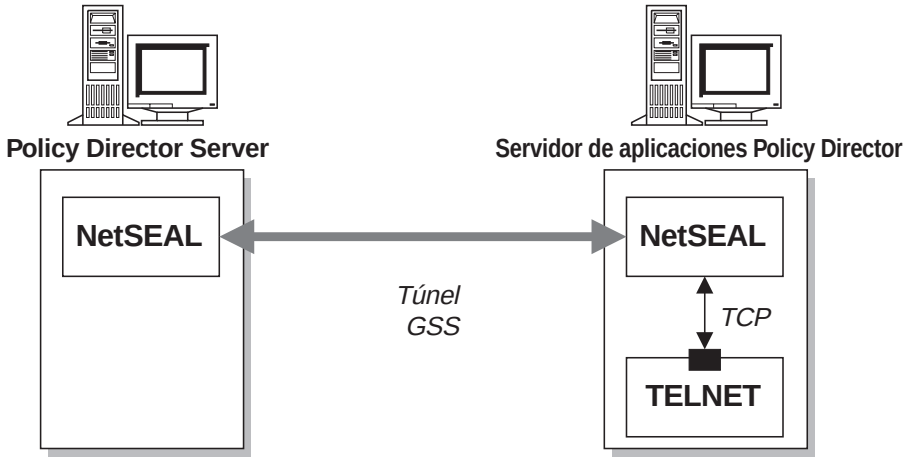
1. ¿Está protegida la puerta solicitada en la máquina de destino (ACL)?

   Sí—Pasar la petición a Security Manager (secmgrd).

   No—Permitir la conexión de salida.
2. ¿Están permitidas las peticiones no autentificadas en la puerta?

   Si—Establecer un túnel seguro con el servidor. Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.



Conexión de salida con sistema principal protegido

TCP puede utilizarse para efectuar una conexión entre un Policy Director NetSEAL Server y un servidor de terceros. No obstante, ninguna de las conexiones efectuadas a través de TCP es segura. No hay ningún NetSEAL Server en el servidor principal de terceros. Policy Director sólo puede permitir o denegar una conexión con el servidor principal; Policy Director no puede asegurar la comunicación a través de la conexión.

El Policy Director Server completa la transacción como sigue:

1. ¿Está protegida la puerta solicitada en la máquina de destino (ACL)?

   Sí—Pasar la petición a Security Manager (secmgrd).

   No—Permitir la conexión de salida.
2. ¿Tiene el usuario permiso para acceder a la puerta solicitada en el servidor de destino?

   Sí—Continuar.

   No—Rechazar la petición de conexión.
3. ¿Se han establecido en la puerta la integridad y la privacidad?

   Sí—Rechazar la petición de conexión.

   No—Establecer una conexión TCP con la puerta solicitada.

Presentación de las conexiones Smart Junction de NetSEAL

Las *conexiones Smart Junction de NetSEAL* proporcionan un mecanismo para enviar con seguridad comunicaciones a un servidor de destino o red a través de una red de servidores Policy Director. Las conexiones (junctions) de NetSEAL determinan la dirección de envío de paquetes a través de un servidor Policy Director.

Las conexiones Smart Junction de NetSEAL son rutas estáticas unidireccionales. Las conexiones Smart Junction unidireccionales permiten al gestor de cada Policy Director Server controlar mejor el acceso a sus redes. Cada dirección de recorrido requiere una conexión (junction) de NetSEAL. Sin embargo, los datos que fluyen a través de una conexión Smart Junction de NetSEAL son siempre bidireccionales.

Un túnel GSS asegura las comunicaciones a través de la conexión Smart Junction de NetSEAL. El Policy Director Server final de la vía de comunicaciones utiliza entonces una conexión TCP con la puerta de destino. Dicha puerta de destino puede estar en el mismo Policy Director Server.

Las conexiones Smart Junction de NetSEAL proporcionan protección y seguridad a los datos en las comunicaciones a través de una empresa. Una empresa puede estar dividida geográfica o funcionalmente. Por ejemplo, las conexiones Smart Junction de NetSEAL son útiles en situaciones en las que existe una red no fiable entre dos Policy Director Servers separados geográficamente. Esos dos Policy Director Servers son miembros de un mismo dominio seguro.

Cada conexión Smart Junction tiene un Policy Director Server de origen, un destino y una dirección de ruta. El destino puede ser otro Policy Director Server o una especificación de red. Las conexiones Smart Junction permiten una fácil configuración de cortafuegos porque todo el tráfico a través de la conexión Smart Junction requiere una sola ruta para atravesar el cortafuego.

Configuración de conexiones Smart Junction de NetSEAL

Un administrador puede crear conexiones Smart Junction de NetSEAL utilizando el programa de utilidad **ivadmin**. El programa de utilidad **ivadmin** contiene mandatos para añadir, eliminar y listar conexiones Smart Junction de NetSEAL. Puede crear conexiones Smart Junction entre Policy Director Servers o entre un Policy Director Server y una red.

Consulte el apartado “Apéndice A. Administración de Policy Director utilizando ivadmin” en la página 279.

Conexiones Smart Junction de NetSEAL y control de accesos

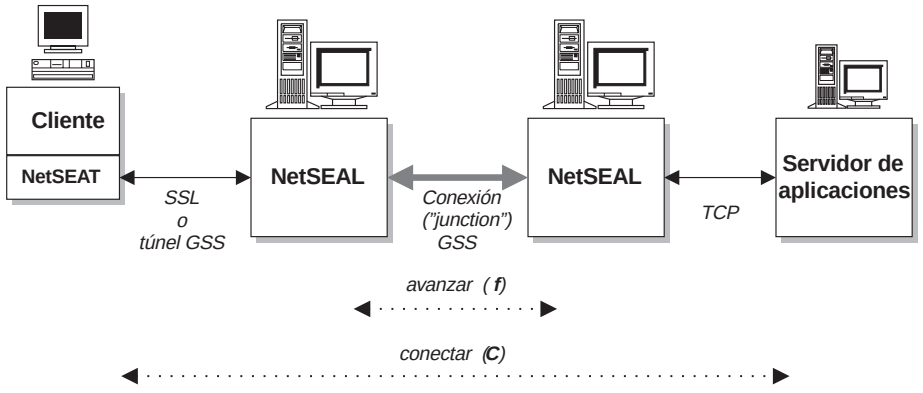
NetSEAL reconoce dos permisos de ACL para controlar el acceso a una puerta de un servidor de aplicaciones.

La ACL de un objeto de puerta de destino controla el acceso a dicha puerta. Una entrada de ACL debe contener el permiso de conectar (C) para permitir que un usuario o grupo acceda a la puerta.

Una ACL de Policy Director Server, responsable de la conexión de salida, controla el avance a través de una conexión Smart Junction de NetSEAL. Una entrada de ACL debe contener el permiso de avanzar (f) para permitir al usuario o grupo el acceso a través de la conexión (junction).

Utilice y compruebe el permiso de avanzar (f) en cada objeto Policy Director Server intermediario de una cadena de servidores conectados con Smart Junction.

Permisos sobre objetos protegidos de NetSEAL:	Acceso	Descripción
C	conexión	Conectar a través de un NetSEAL Server con un servicio protegido local o remoto
f	avanzar	Permitir una conexión de salida a través de una conexión (junction) NetSEAL; atravesar la conexión (junction)



Descripción de los servicios controlados por conexiones Smart Junction de NetSEAL

Las conexiones Smart Junction de NetSEAL proporcionan protección y seguridad a los datos en las comunicaciones a través de una empresa. Una empresa puede estar dividida geográfica o funcionalmente. Por ejemplo, las conexiones Smart Junction de NetSEAL son útiles en situaciones en las que existe una red no fiable entre dos Policy Director Servers separados geográficamente. Esos dos Policy Director Servers son miembros de un mismo dominio seguro.

Los ejemplos son los siguientes:

- "Conexión Smart Junction entrante con Policy Director Server".
- "Conexión Smart Junction entrante con sistema principal protegido" en la página 241.
- "Conexión de salida con Policy Director Server conectado con Smart Junction" en la página 241.
- "Conexión de salida con sistema principal protegido conectado con Smart Junction" en la página 242.

Conexión Smart Junction entrante con Policy Director Server

Este ejemplo presenta una aplicación que reside en un Policy Director Server remoto protegido. En este ejemplo se establece explícitamente el túnel (tunnel) GSS entre los servidores Policy Director como conexión Smart Junction de NetSEAL. En el control de acceso a la puerta de destino se tiene ahora en cuenta el permiso de avanzar.

El Policy Director Server completa la transacción como sigue:

1. ¿Puede conectar el usuario con la puerta solicitada del servidor de destino (basándose en la ACL)?

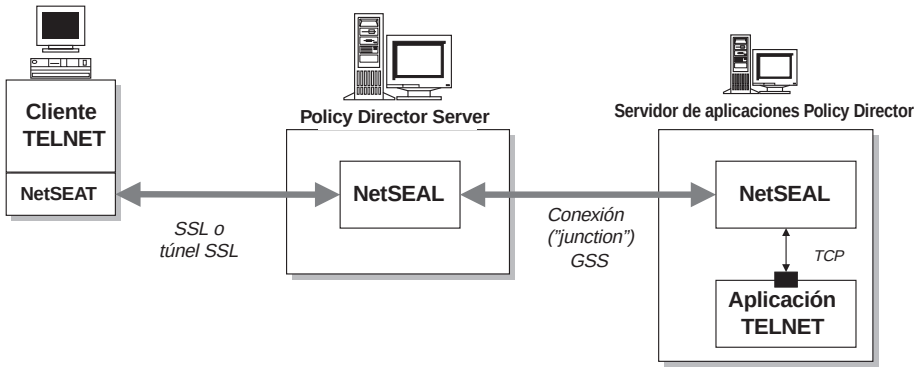
   Sí—Continuar.

   No—Rechazar la petición de conexión.

2. ¿Puede el usuario avanzar a través de la conexión Smart Junction?

   Sí—Hacer avanzar la petición a través de la conexión (junction) GSS. Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.



Conexión Smart Junction entrante con sistema principal protegido

Este ejemplo presenta una aplicación que reside en un servidor remoto, de terceros, protegido. En este ejemplo se establece explícitamente el túnel (tunnel) GSS entre los servidores Policy Director como conexión Smart Junction de NetSEAL. En el control de acceso a la puerta de destino se tiene ahora en cuenta el permiso de avanzar.

El Policy Director Server completa la transacción como sigue:

1. ¿Puede conectar el usuario con la puerta solicitada del servidor de destino (basándose en la ACL)?

   Sí—Continuar.

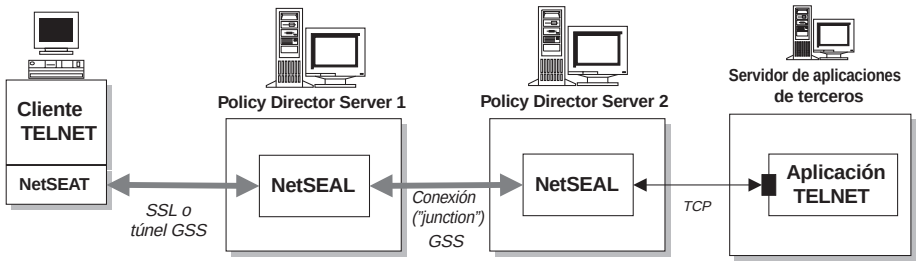
   No—Rechazar la petición de conexión.

2. ¿Puede el usuario avanzar a través de la conexión Smart Junction?

   Sí—Hacer avanzar la petición a través de la conexión (junction). Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.

Un servidor de aplicaciones de terceros tiene siempre una conexión TCP desprotegida. Utilice una configuración de este tipo en un entorno de red fiable.



Conexión de salida con Policy Director Server conectado con Smart Junction

Este ejemplo presenta una aplicación que reside en un Policy Director Server remoto protegido. En este ejemplo se establece explícitamente el túnel (tunnel) GSS entre los servidores Policy Director como conexión Smart Junction de NetSEAL. En el control de acceso a la puerta de destino se tiene ahora en cuenta el permiso de avanzar, que proporciona una buena protección para servidores de la gama media.

El Policy Director Server completa la transacción como sigue:

1. ¿Está protegida la puerta solicitada en la máquina de destino (ACL)?

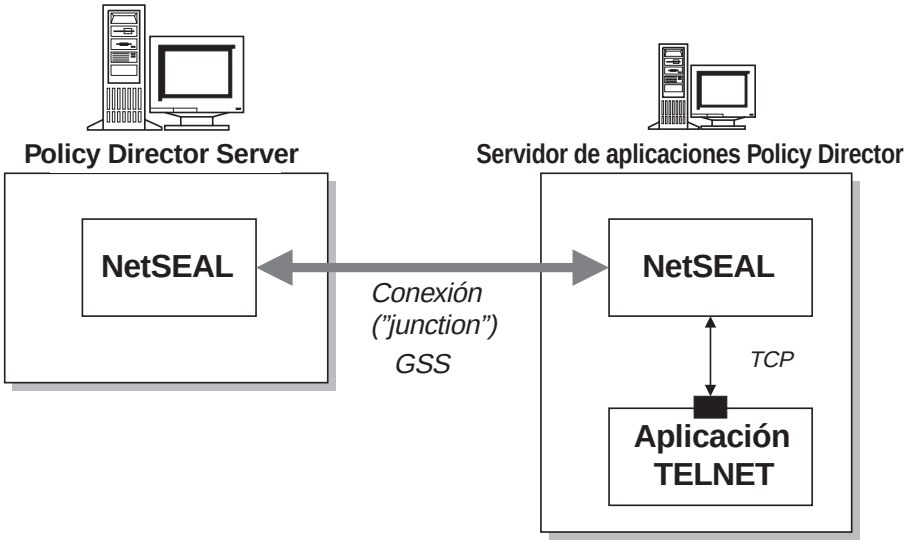
   Sí—Pasar la petición a Security Manager (secmgrd).

   No—Permitir la conexión de salida.

2. ¿Puede el usuario avanzar a través de la conexión Smart Junction?

   Sí—Hacer avanzar la petición a través de la conexión (junction). Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.



Conexión de salida con sistema principal protegido conectado con Smart Junction

Este ejemplo presenta una aplicación que reside en un servidor remoto, de terceros, protegido. En este ejemplo se establece explícitamente el túnel (tunnel) GSS entre los servidores Policy Director como conexión Smart Junction de NetSEAL. En el control de acceso a la puerta de destino se tiene ahora en cuenta el permiso de avanzar.

El Policy Director Server completa la transacción como sigue:

1. ¿Está protegida la puerta solicitada en la máquina de destino (ACL)?

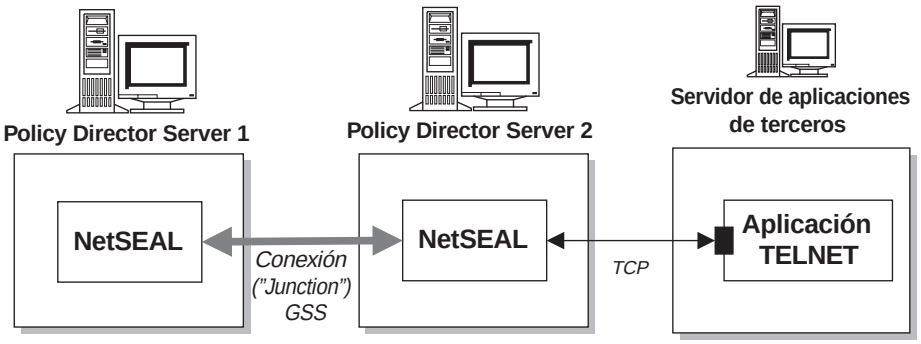
   Sí—Pasar la petición a Security Manager (secmgrd).

   No—Permitir la conexión de salida.

2. ¿Puede el usuario avanzar a través de la conexión Smart Junction?

   Sí—Hacer avanzar la petición a través de la conexión (junction). Establecer una conexión TCP con la puerta solicitada.

   No—Rechazar la petición de conexión.



Protección de servicios TCP

Las ACL de las puertas de servicio TCP controlan el acceso a dichas puertas. Un cliente NetSEAL puede acceder a un servicio TCP específico cuando la ACL del objeto de puerta contiene el permiso de conectar (C) para el usuario.

Un administrador puede denegar el acceso al servicio TCP eliminando simplemente el permiso de conexión de la entrada adecuada de la ACL.

Los permisos ACL también pueden controlar la calidad de la protección de la comunicación NetSEAL. Algunas combinaciones de los permisos de integridad y privacidad de los datos determinan la calidad de la protección. La calidad de la protección de la comunicación de salida puede controlarse mediante una conexión Smart Junction de NetSEAL. Para controlar la calidad de la protección, las entradas de la ACL en el objeto de puerta de destino deben contener el permiso de integridad y el permiso de privacidad.

La ACL probada es la más específica dependiendo de la dirección de red y la máscara de red del objeto. La presencia o ausencia de una ACL en una puerta de destino no se tiene en cuenta cuando se localiza el objeto solicitado en el cual debe realizarse la comprobación de ACL.

Por ejemplo, a un cliente que utiliza TELNET para comunicarse 10.0.0.1 cuando están configuradas las siguientes ACL se le permitirá el acceso según la ACL3. Policy Director permite el acceso aunque la puerta 23 de la red coincidente contiene una ACL explícita.

`10.0.0.0:255.255.255.0`	ACL1
`10.0.0.0:255.255.255.0/Puerta 23`	ACL2
`10.0.0.1:255.255.255.255`	ACL3

Capítulo 18. NetSEAL: Tareas generales de administración

NetSEAL es una solución de Virtual Private Network (VPN) para asegurar las comunicaciones entrantes TCP/IP. Como gestor de recursos, NetSEAL controla la posibilidad por parte de un usuario de conectarse con una aplicación específica TCP. Este capítulo contiene información que describe las tareas generales de administración que pueden realizarse para personalizar NetSEAL para la red.

Este capítulo incluye los siguientes temas:

Habilitación e inhabilitación de la seguridad de NetSEAL

Utilice el programa de utilidad **ivadmin** para habilitar e inhabilitar NetSEAL.

Habilitación de NetSEAL

Para habilitar NetSEAL en un servidor específico de Policy Director:

```
ivadmin>
server enable /NetSEAL/nombre sistema principal
```

Donde *nombre sistema principal* es el nombre del sistema principal del servidor excluyendo el nombre de dominio.

Cuando el servicio ya se ha habilitado o cuando la especificación de servicio no es válida, Policy Director devuelve errores.

Policy Director inhabilita NetSEAL por omisión a menos que se instale el componente de detección de NetSEAL (IVTrap) de la distribución de Policy Director.

Inhabilitación de NetSEAL

Para inhabilitar NetSEAL en un servidor específico de Policy Director:

```
ivadmin>
server disable /NetSEAL/nombre sistema principal
```

Estado de NetSEAL

Para comprobar el estado de NetSEAL Server, utilice el mandato **server status**:

```
ivadmin> server status
/NetSEAL/nombre sistema principal
```

El informe de estado visualiza la siguiente información:

- Si el servidor WebSEAL está inhabilitado o inhabilitado.
- Si el servidor NetSEAL está disponible.
- Si las réplicas de bases de datos de configuración de NetSEAL se han actualizado.

Utilización de controles de acceso de NetSEAL

Las conexiones NetSEAL disponen de los permisos de ACL de Policy Director para los siguientes factores de seguridad:

- Permitir el acceso a servicios TCP como, por ejemplo, puertas de destino
- Permitir el envío de paquetes a través de conexiones Smart Junction de NetSEAL
- Asegurar la integridad y la privacidad de los datos

La ACL de un objeto de puerta de destino controla el acceso a dicha puerta. Una entrada de ACL debe contener el permiso de conectar (C) para permitir que un usuario o grupo acceda a la puerta. El permiso de conexión también puede regir el acceso a un servidor de aplicaciones de una red protegida.

Una ACL de Policy Director Server, responsable de la conexión de salida, controla el avance a través de una conexión Smart Junction de NetSEAL. Una entrada de ACL debe contener el permiso de avanzar (f) para permitir al usuario o grupo el acceso a través de la conexión (junction).

Utilice y compruebe el permiso de avanzar (f) en cada objeto Policy Director Server intermediario de una cadena de servidores conectados con Smart Junction.

	Acceso	**Descripción**
C	conexión	Conectar a través de un NetSEAL Server con un servicio protegido local o remoto
f	avanzar	Permitir una conexión de salida a través de una conexión (junction) NetSEAL; atravesar la conexión (junction)

Los permisos ACL también pueden controlar la calidad de la protección de la comunicación NetSEAL. Algunas combinaciones del permiso de integridad de los datos y del permiso de privacidad de los datos determinan la calidad de la protección.

La calidad de la protección de la comunicación de salida puede controlarse mediante una conexión Smart Junction de NetSEAL. Las entradas de la ACL del objeto de puerta de destino deben contener los permisos de integridad (I) y privacidad (P). La integridad y privacidad de los datos no pueden ampliarse a un servidor de aplicaciones de terceros (no Policy Director) en una red fiable.

Gestión de redes protegidas

Se puede pensar en las redes como si fuesen servidores no Policy Director protegidos por NetSEAL. Utilice el programa de utilidad **ivadmin** para definir y gestionar las redes. Este programa incluye mandatos para añadir, eliminar y listar redes protegidas.

Mandato	**Descripción**
netseal network add *red máscara red* **[***alias red***]**	

	Crear una nueva red que debe proteger NetSEAL. El par red / máscara de red son números de dirección estándar de red IP y máscaras de red. El nombre de alias de red opcional puede utilizarse para identificar la red. Si no se especifica ningún alias, la red debe identificarse mediante el par de red y máscara de red. Se recibirán errores si la red ya existe.
netseal network delete *id-red*	
	Elimine del sistema la red especificada; *id-red* puede corresponder a uno de los siguientes elementos: • par *red/máscara de red* • *alias de red* El argumento id-red puede corresponder a un par de red / máscara de red o a un alias de red. Todas las referencias a esta red del sistema se suprimirán, incluidas las conexiones Smart Junction de NetSEAL. Se recibirá un error si la red no se encuentra dentro de la base de datos.
netseal network list	
	Visualiza todas las redes de la base de datos, lo que incluye el par de red y máscara de red así como todos los alias definidos.

Ejemplo:

```
ivadmin> netseal network add 10.125.0.0 255.255.255.0 west
```

Este mandato añado los nodos de red del 10.125.0.0 al 10.125.0.255 a una especificación de red protegida por NetSEAL. Este mandato también asigna a esta especificación de red el nombre de alias `west`.

Gestión de conexiones Smart Junction de NetSEAL

Las conexiones Smart Junction de NetSEAL determinan en qué dirección debe ir la comunicación a través de un Policy Director Server. Pueden crearse conexiones Smart Junction entre dos Policy Director Servers o entre un Policy Director Server y una red. La utilización de un túnel GSS asegura la comunicación a través de una conexión Smart Junction entre dos Policy Director Servers.

Utilice el programa de utilidad **ivadmin** para definir y gestionar conexiones Smart Junction de NetSEAL. Este programa incluye mandatos para añadir, eliminar y listar conexiones Smart Junction de NetSEAL.

Mandato	**Descripción**
netseal junction add *nombre sistema principal destino*	
	Crea una conexión (junction) de un NetSEAL Server a un destino especificado en el que *nombre sistema principal* es el nombre del NetSEAL Server menos el nombre del dominio, y *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Se reciben errores si la conexión (junction) ya existe, el servidor del sistema principal no existe o el destino no existe.
netseal junction delete *nombre sistema principaldestino*	

	Elimina la conexión (junction) de un NetSEAL Server con el destino especificado, siendo *nombre sistema principal* el nombre del NetSEAL Server menos el nombre de dominio; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Se recibe un error si la conexión Smart Junction no existe. El mandato no tiene ningún efecto en las conexiones actuales.
netseal junction list *nombre sistema principal*	
	Visualiza todas las conexiones Smart Junction de NetSEAL para el NetSEAL Server especificado.

Ejemplo:

```
ivadmin> netseal junction add
clipper west
```

Este mandato crea una conexión Smart Junction desde el NetSEAL Server `clipper` a la red definida con el alias `west`. El mandato también define la dirección de ruta (de `clipper` a `west`); las conexiones Smart Junction de NetSEAL son unidireccionales.

Gestión de puertas protegidas

Policy Director NetSEAL Server proporciona servicios de seguridad para puertas, sistemas principales y redes específicos. Por ejemplo, NetSEAL Server puede configurarse para asegurar el tráfico de TELNET en una puerta determinada.

Utilice el programa de utilidad **ivadmin netseal** para definir la lista de puertas que desee que NetSEAL proteja. Este programa incluye mandatos para añadir, eliminar y listar puertas protegidas. Pueden especificarse puertas para Policy Director Servers o redes.

Mandato	Descripción
netseal port add *destino id-puerta*	
	Protege conexiones con el destino especificado en el *id-puerta* indicado; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • *red máscara de red* • *alias de red* El *id-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* • *alias de puerta* Se recibe un error si la puerta ya está protegida, si el servidor no existe o el alias de puerta no existe.
netseal port delete *destino id-puerta*	

	Detiene la protección de conexiones con el destino especificado en la puerta especificada; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • *red máscara de red* • *alias de red* E *id-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* • *alias de puerta* Se recibe un error si la puerta no está protegida aún, si el servidor no existe o el alias de puerta no existe.
netseal port list *destino*	
	Visualiza una lista de todas las puertas del destino especificado; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • *red máscara de red* • *alias de red* Se recibe un error si el servidor no existe.

Nota: Indique el rango de puertas con dos números separados por un guión (por ejemplo: 22–88).

Ejemplo:

```
ivadmin> port add west 23
```

Este mandato define el número de puerta 23 en la red especificada mediante el alias de red “west” como puerta protegida por NetSEAL.

Gestión de alias de puertas protegidas

Utilice el programa de utilidad **ivadmin** para definir y gestionar alias de puertas. Este programa incluye mandatos para añadir, eliminar y listar alias de puertas. Utilice los alias de puertas para identificar rangos de puertas detectados de una forma de que tenga más sentido.

Mandato	Descripción
netseal port-alias add *espec-puerta alias-puerta*	
	Crear un nuevo alias de puerta para la especificación de puerta; *espec-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* Recibirá un error si el rango de puertas ya tiene otro alias.
netseal port-alias delete *id-puerta*	
	Eliminar del sistema el alias de puerta del id-puerta especificado; *id-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* • *alias de puerta* Se recibirá un error si el alias de puerta no se encuentra dentro de la base de datos.

netseal port-alias list	
	Visualizar todos los alias de puerta que se encuentran dentro de la base de datos.

Ejemplos:

```
ivadmin> netseal port-alias add 23 telnet
```

Este mandato crea el alias de puerta `telnet` para la puerta número 23.

```
ivadmin> netseal port-alias add 5000-5010 pilot
```

Este mandato crea el alias de puerta “pilot” para el rango de puertas 5000 a 5010.

Configuración de sistemas principales fiables y redes fiables

Policy Director NetSEAL Server proporciona servicios de seguridad para puertas, sistemas principales y redes específicos. Por ejemplo, NetSEAL Server puede configurarse para asegurar el tráfico de TELNET en una puerta determinada del Policy Director Server. Además, NetSEAL Server puede considerar fiables determinados sistemas (sistemas principales fiables) y determinados grupos de sistemas principales (redes fiables).

Las secciones `[trusted_hosts]` o `[trusted_networks]` del archivo de configuración secmgrd.conf contienen parámetros para identificar sistemas principales fiables y redes fiables.

Sistemas principales fiables

Su NetSEAL Server se comunica frecuentemente con determinados sistemas principales altamente fiables. Puede optimizar el rendimiento permitiendo a NetSEAL exima a las peticiones entrantes de esos servidores del control de acceso.

Nota: La identificación de sistemas principales fiables deja vulnerable a su sistema ante intentos de engaño a través de IP. Asegúrese de proteger todos los sistemas principales contra ataques de este tipo.

Por omisión, Policy Director no identifica los sistemas principales fiables.

Para identificar un sistema principal fiable, vaya a la sección `[trusted_hosts]` y liste la dirección IP y el nombre del servidor.

Por ejemplo, para considerar fiables todas las peticiones de un servidor llamado “typhoon” con la dirección IP 220.12.35.102, escriba:

```
[trusted_hosts]
220.12.35.102 = typhoon
```

Cuando se utiliza la detección de NetSEAL para asegurar una máquina, acostumbra a ser necesario considerar fiable la máquina local. Al considerar fiable la máquina local, se permite a los servicios que se ejecutan en la máquina seguir funcionando. Los servicios continúan funcionando incluso si el acceso no autentificado está desactivado para una puerta o un rango de puertas.

Policy Director necesita estas entradas para poder *considerar fiable* la máquina local:

- Una entrada para el sistema principal local
- Entradas para cada dirección IP asociada a la máquina

Por ejemplo, el NetSEAL Server typhoon podría tener la dirección IP 220.12.35.102. Otro proceso del mismo servidor podría tener la dirección IP de sistema principal 127.0.0.1. Para considerar fiables todas las peticiones locales del NetSEAL Server typhoon procedentes de otros procesos del mismo servidor, debería escribir:

```
[trusted_hosts]
220.12.35.102 = typhoon
127.0.0.1 = localhost
```

Normalmente hay una sola dirección IP por máquina, sin embargo, algunas máquinas están conectadas a más de una red y, por lo tanto, tiene más de una dirección.

Redes fiables

Si su red tiene subredes enteras o redes de área loca de sistemas fiables, podrá especificar toda la subred sin necesidad de tener que indicar cada sistema principal.

Por omisión, Policy Director no define ninguna red fiable.

Para identificar una red fiable, vaya a la sección `[trusted_networks]` y liste la máscara de red y dirección IP de la subred.

Por ejemplo, para considerar fiables todas las peticiones de la subred 192.96.32.0, escriba:

```
[trusted_networks]
192.96.32.0 = 255.255.255.0
```

Definición de los parámetros de tiempo de espera de SSL

Pueden definirse los siguientes parámetros de tiempo de espera de SSL:

- "Definición del tiempo de espera en antememoria de sesión SSL".
- "Definición del tiempo de espera de conexiones SSL" en la página 252.

Definición del tiempo de espera en antememoria de sesión SSL

La sección `[ssl]` del archivo de configuración secmgrd.conf contiene el parámetro para definir el tiempo de espera estático de antememoria de sesión SSL.

NetSEAL coloca internamente en la antememoria la información sobre credenciales. El parámetro de tiempo de espera en la antememoria de la sesión indica el periodo de tiempo que la información sobre credenciales de autorización permanece en la memoria de NetSEAL.

Este parámetro no indica un tiempo de espera por inactividad. El valor se correlaciona con un *tiempo de vida de credencial* en vez de con un *tiempo de espera de credencial*. Su finalidad es mejorar la seguridad al forzar al usuario a volver a autentificarse cuando se alcanza el límite de tiempo de espera especificado.

El tiempo de espera en la antememoria (en segundos) por omisión es:

```
[ssl]
tiempo-espera-antememoria-ssl = 3600
```

Ajuste este valor para equilibrar el rendimiento del servidor a conveniencia del usuario, dependiendo del volumen de peticiones SSL que debe gestionar el servidor.

Definición del tiempo de espera de conexiones SSL

La sección [ssl] del archivo de configuración secmgrd.conf contiene el parámetro para definir el tiempo de espera de conexión de SSL.

Cuando NetSEAL acepta una conexión SSL de un cliente NetSEAT a través de un túnel (tunnel) SSL de NetSEAL, es necesario que se produzca una reconocimiento del protocolo de SSL. Este parámetro controla el tiempo que Security Manager espera a que NetSEAT inicie un reconocimiento de SSL al principio de una conexión SSL. Transcurrido este tiempo, Security Manager cierra la conexión.

El tiempo de espera de conexión de SSL por omisión (en segundos) es:

```
[ssl]
ssl-init-connect-timeout = 120
```

Asignación de conexiones de NetSEAL

Los parámetros para asignar conexiones NetSEAL se encuentran en la sección [netseal] del archivo de configuración secmgrd.conf.

Utilice max-connections para especificar el número máximo de conexiones simultáneas que va a permitir NetSEAL.

La instalación de Policy Director establece el siguiente valor por omisión:

```
[netseal]
max-connections = 32
```

Si lo desea, puede aumentar este valor para que se ajuste mejor a las condiciones de tráfico de su red. Si el valor de max-connections es demasiado bajo, las conexiones se rechazarán cuando en condiciones en que la carga sea alta. Si el valor es demasiado alto, se malgastarán recursos y el rendimiento del servidor se degradará.

Nota: El límite inferior de este parámetro de configuración es 20. Si intenta definir un valor inferior a 20, dicho valor adoptará simplemente el valor por omisión 20.

Capítulo 19. NetSEAT: Visión general

El cliente Policy Director NetSEAT permite a los clientes Windows participar del dominio seguro de Policy Director. NetSEAT proporciona un túnel seguro entre clientes Windows y Policy Director Servers. NetSEAT cifra las comunicaciones utilizando la tunelización (″tunnel″) de SSL o GSS.

Este capítulo incluye los siguientes temas:

Presentación del cliente NetSEAT

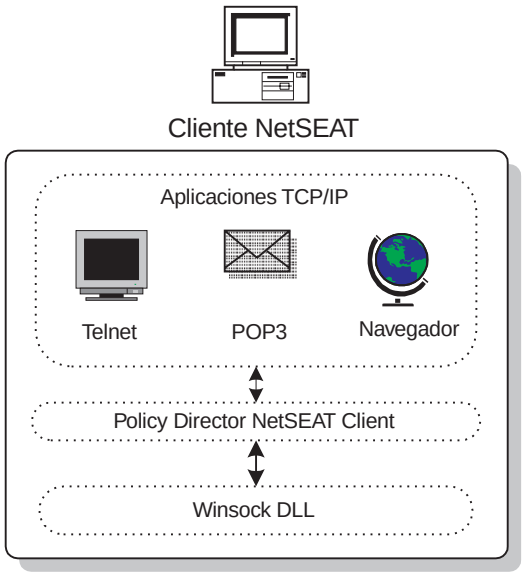
El cliente Policy Director NetSEAT permite a los clientes Windows comunicarse de forma segura con servidores WebSEAL y NetSEAL de Policy Director. Añadiendo NetSEAT a una estación de trabajo Windows se configura la estación de trabajo para un dominio seguro de Policy Director. Un dominio seguro es aquél en el que NetSEAT puede utilizar los servicios de seguridad de autentificación y autorización de Policy Director.

NetSEAT permite la autentificación y la protección de mensajes a nivel de protocolo de red. Para poder utilizar NetSEAT, no es necesario volver a compilar o enlazar una aplicación.

NetSEAT asegura el tráfico de la red entre el cliente Windows y un servidor Policy Director al interceptar las peticiones de la red antes de que atraviesen la capa de Winsock. NetSEAT utiliza su información de configuración para reconocer las peticiones efectuadas desde aplicaciones TCP/IP genéricas. Entre las aplicaciones TCP/IP genéricas se encuentran TELNET, POP3 o HTTP.

Cuando se efectúa una petición de cliente a una aplicación de un Policy Director Server, NetSEAT establece de forma transparente un túnel seguro con el Policy Director Server. A continuación, NetSEAT redirige las peticiones del cliente a través del túnel.

NetSEAT asegura y cifra las comunicaciones con un Policy Director Server utilizando uno de dos métodos: un túnel SSL o un túnel GSS. Un túnel SSL utiliza SSL para cifrar la comunicación. Un túnel GSS utiliza la API de GSS para cifrar la comunicación.



Configuraciones soportadas

El cliente NetSEAT puede utilizarse con varias finalidades, como se explica en:

- "Cliente de Virtual Private Network".
- "Módulo de soporte para Policy Director en Windows NT".
- "Módulo de soporte para Policy Director Management Console" en la página 255.

Cliente de Virtual Private Network

NetSEAT puede configurarse como cliente de Virtual Private Network (VPN) que utilice un túnel seguro para proporcionar un enlace de comunicaciones seguras con un Director NetSEAL Server.

Como cliente de VPN, NetSEAT puede cifrar las comunicaciones utilizando los siguientes tipos de túneles:

- SSL
- GSS

Módulo de soporte para Policy Director en Windows NT

Policy Director instala NetSEAT como módulo de soporte para cada instalación de los componentes del servidor de Policy Director para Windows NT. Policy Director para Solaris y AIX no requiere este soporte del cliente NetSEAT.

Con esta función, el cliente NetSEAT proporciona una detección de kernel para que la utilicen internamente los servicios de seguridad (Security Services) de Policy Director.

Como módulo de soporte de Policy Director para Windows NT, NetSEAT necesita los siguientes servicios:

- Directory Services Broker
- Tunelización (″tunnel″) de GSS

Utilice la tunelización de GSS cuando instale el cliente NetSEAT como módulo de soporte para Policy Director para Windows NT o Policy Director Management Console en Windows.

Módulo de soporte para Policy Director Management Console

Cuando se ejecuta Policy Director Management Console en un cliente Windows, debe instalarse NetSEAT como módulo de soporte. En esta configuración , NetSEAT habilita un administrador para utilizar Management Console a fin de realizar tareas administrativas desde un sistema Windows. El sistema Windows no debe tener instalado ninguno de los componentes de Policy Director Server.

Como módulo de soporte de Management Console, NetSEAT necesita los siguientes servicios:

- Directory Services Broker
- tunelización (″tunnel″) de GSS

Utilice la tunelización de GSS cuando instale el cliente NetSEAT como módulo de soporte para Policy Director para Windows NT o Policy Director Management Console en Windows.

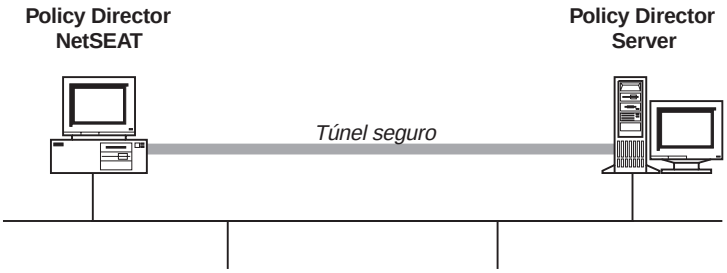
Tunelización segura

Antes de enviar una petición de cliente, NetSEAT utiliza un túnel seguro para ponerse en contacto con Policy Director Security Server (para saber cuál es el dominio seguro adecuado). NetSEAT utiliza también un túnel seguro para establecer la identidad y las cliente del cliente. Si la autentificación es satisfactoria, NetSEAT encapsula la transacción solicitada en otro túnel seguro. Asimismo, NetSEAT 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 asegurado por WebSEAL, NetSEAT intercepta de forma transparente la petición. Si esta es la primera petición a Policy Director y necesita una autentificación, NetSEAT visualiza para el usuario un recuadro de diálogo de inicio de sesión.

Cuando Policy Director ha autentificado al usuario, NetSEAT permite de forma transparente las peticiones siguientes y los túneles seguros basados en las credenciales iniciales. NetSEAT utiliza las credenciales para tomar decisiones de autorización para cada petición.

NetSEAT puede establecer dos tipos distintos de túneles seguros, como se explica en los apartados “Utilización de la tunelización de SSL” y “Utilización de la tunelización de GSS” en la página 256.



Utilización de la tunelización de SSL

El término *tunelización de SSL* se refiere a un túnel seguro que utiliza el protocolo SSL. NetSEAT utiliza la tunelización (″tunnel″) cuando se utiliza como cliente VPN para Policy Director NetSEAL. La utilización del túnel SSL simplifica la

configuración de NetSEAT. En ese caso, no es necesario el administrador especifique la configuración de los servicios DCE dentro del dominio seguro de Policy Director.

Un túnel SSL también resulta útil cuando un cliente desea acceder a datos protegidos por un cortafuego. En esta modalidad, NetSEAT emplea una sola puerta para todas las comunicaciones con Policy Director que se encuentren detrás del cortafuego. Policy Director encapsula todas las comunicaciones que pasan a través de la puerta en un túnel seguro.

Durante la configuración de NetSEAT, puede especificar el número de puerta que desea utilizar para atravesar el cortafuego. El número de la puerta debe coincidir con el número de puerta configurado en el NetSEAL Server.

La tunelización de SSL puede ser utilizada por usuarios autentificados a través del un registro de usuarios LDAP o de un registro de usuarios DCE.

Utilización de la tunelización de GSS

El término *tunelización de GSS* se refiere a un túnel seguro basado en la utilización de la API de Generic Security Service (GSS API). NetSEAT usa un túnel GSS cuando se comunica con células DCE.

En esta modalidad, NetSEAT es un cliente que utiliza Security Managers (secd) y Time Servers (dtsd) situados en otros servidores de la célula DCE. NetSEAT también utiliza Policy Director Directory Services Broker para las peticiones de búsqueda del espacio de nombres proxy a los Cell Directory Services (cdsd) situados en otro lugar de la célula DCE.

Un túnel GSS seguro se utiliza al integrar un inicio de sesión PKI de un usuario, a través de un cliente Entrust con la identidad del usuario en el dominio seguro de Policy Director. En este caso, los usuarios inician la sesión con su estación de trabajo utilizando un cliente Entrust PKI. Cuando el usuario intenta utilizar los servicios de autentificación y autorización de Policy Director, se establece un túnel seguro entre NetSEAT y los servidores de Policy Director. Los servidores de Policy Director correlacionan automáticamente la identidad de inicio de sesión con la identidad del usuario de Policy Director para poder tomar decisiones de autentificación y autorización.

La tunelización de GSS no puede utilizarse para usuarios autentificados por un registro de usuarios LDAP.

Acceso a servicios protegidos

Un cliente NetSEAT puede utilizar el túnel seguro a un Policy Director NetSEAL Server para enviar peticiones a cualquier servidor de aplicaciones remoto. Estos servidores de aplicaciones remotos están protegidos por el NetSEAL Server. Durante la configuración de NetSEAT el administrador puede especificar:

- El nombre del servidor de aplicaciones.
- El NetSEAL Server que lo protege.
- El tipo de túnel seguro (túnel SSL o GSS) que se utiliza entre NetSEAT y NetSEAL.

Cuando está configurado con esta información, NetSEAT intercepta las peticiones del cliente Windows al servidor de aplicaciones. A continuación, NetSEAT las dirige a un Policy Director NetSEAL Server a través de un túnel seguro .

También puede configurar NetSEAT para que acceda a las subredes protegidas completas si están protegidas por Policy Director NetSEAL. Un ejemplo de esto podría ser una intranet protegida desde Internet por un Policy Director NetSEAL Server.

Directory Services Broker

Cuando se utiliza como módulo de soporte para Policy Director Servers y Management Console en Windows (tunelización de GSS), NetSEAT requiere los servicios de un Directory Services Broker (DSB). Se necesita un DSB para comunicar con los Policy Director Servers. El espacio de nombres de proxys de DSB busca un servidor de Cell Directory Services que se encuentre en el mismo dominio seguro.

Policy Director instala automáticamente el DSB como parte del paquete Policy Director Management Server (IVMgr). El cliente NetSEAT debe configurarse de forma que conozca el nombre del sistema servidor que sea el sistema principal de Directory Services Broker.

Capítulo 20. NetSEAT: Tareas generales de administración

Este capítulo describe las tareas de administración del sistema para configurar el cliente NetSEAT gestionando contextos de seguridad y buscando y corrigiendo problemas (*resolución de problemas*).

Este capítulo incluye los siguientes temas:

Configuración del cliente NetSEAT

Configure cada cliente NetSEAT en un dominio seguro de Policy Director. Puede configurar los clientes NetSEAT durante la instalación o en cualquier otro momento después de ésta. La herramienta de NetSEAT Configuration (programa de utilidad) proporciona una interfaz gráfica de usuario que permite a los administradores configurar fácilmente el cliente.

Realice todas las tareas de configuración dentro del contexto de un dominio seguro y configure NetSEAT para que participe de dicho dominio seguro.

Algunas tareas de configuración se aplican únicamente a configuraciones de uno de los tipos de túneles seguros (GSS or SSL). NetSEAT utiliza estos túneles seguros para comunicarse con Policy Director Servers. Los clientes NetSEAT, configurados para ser únicamente clientes SSL para NetSEAL Servers, requieren únicamente un subconjunto limitado de las tareas de configuración.

La siguiente tabla indica qué tareas de configuración corresponden a cada tipo de túnel seguro:

Tipos de túnel	Tareas de configuración
GSS y SSL	• "Adición de NetSEAT a un dominio seguro" en la página 260 • "Configuración de NetSEAL Servers" en la página 263 • "Denegación de acceso a los recursos de red" en la página 270

Sólo GSS	• "Adición de DCE Servers" en la página 261 • "Definición de las propiedades del DCE Server" en la página 262 • "Configuración de un inicio de sesión integrado" en la página 265 • "Configuración del inicio de sesión avanzado (integración PKI)" en la página 268. • "Definición del delta de tiempo máximo" en la página 270
Sólo SSL	"Configuración de un proxy SSL" en la página 270

NetSEAT proporciona derivaciones para varios programas de utilidad de seguridad de DCE y facilita también un programa de utilidad para comprobar la disponibilidad de los servicios DCE.

Estos programas de utilidad sólo se utilizan cuando se configura NetSEAT para que utilice la tunelización (″tunnel″) de GSS.

Las siguientes secciones describen estos programas de utilidad:

- Utilización de programas de utilidad de seguridad de NetSEAT (consulte el apartado "Utilización de los programas de utilidad de seguridad de NetSEAT" en la página 271).
- Búsqueda y corrección de problemas utilizando **netseat_ping** (consulte el apartado "Resolución de problemas con netseat_ping" en la página 273.)

Inicio de la herramienta NetSEAT Configuration

Para volver a configurar NetSEAT después de haber finalizado la instalación y configuración iniciales, utilice la herramienta de configuración de NetSEAT (NetSEAT Configuration). Si ha pospuesto la configuración de NetSEAT durante la instalación inicial, utilice también la herramienta de configuración de NetSEAT para configurarlo.

La herramienta de configuración de NetSEAT (NetSEAT Configuration) puede iniciarse de dos formas:

- Para iniciar la herramienta NetSEAT Configuration desde el escritorio de Windows, pulse el botón en **Inicio → Programas → Policy Director → NetSEAT → Configuración de NetSEAT**
- Para iniciar la herramienta de configuración de NetSEAT desde el icono **NetSEAT** de la Bandeja del sistema, pulse el botón derecho del ratón en el icono **NetSEAT** y seleccione **Propiedades**.

Adición de NetSEAT a un dominio seguro

Para añadir NetSEAT a un dominio seguro, realice los siguientes pasos:

1. Inicie la herramienta NetSEAT Configuration. Al iniciarse, la herramienta de configuración de NetSEAT, visualiza el separador **Dominios seguros** en la ventana de configuración de NetSEAT.
2. Pulse el botón en **Añadir**.

   Aparecerá el recuadro de diálogo Nuevo dominio seguro.
3. Escriba el nombre del dominio seguro al que pertenece NetSEAT.
4. Seleccione los protocolos soportados en ese dominio y pulse el botón en **Aceptar**.

- Si seleccionó **Habilitar GSS**, vaya al apartado “Adición de DCE Servers” .
- Si seleccionó **Habilitar sólo SSL**, vaya al apartado “Configuración de NetSEAL Servers” en la página 263.

5. **Sólo tunelización GSS**—Si ha configurado más de un dominio, vuelva al separador **Dominios seguros**. Resalte el dominio por omisión para los inicios de sesión del usuario. A continuación, pulse el botón en **Definir como omisión**.

   Si sólo ha configurado un dominio, éste se convierte automáticamente en el dominio por omisión.
6. Pulse el botón en **Aceptar**.

Adición de DCE Servers

Si configura un dominio para habilitar la utilización de un túnel seguro de GSS, deberá definir otras opciones de configuración.

Para el dominio seguro (o *célula*) al que se conecta NetSEAT, obtenga el nombre de los sistemas Policy Director Security Server de la célula. Identifique los servicios básicos de seguridad (DCE) proporcionados por cada sistema. Para cada servidor, indique si proporciona:

- **Seguridad** — Security Services (secd)
- **Hora** — Time Services (dtsd)
- **DSB** — Directory Services Brokers (dsb)
- **CDS** — Cell Directory Services (cdsd)

  NetSEAT sólo necesita conocer la ubicación de Cell Directory Services (CDS) si Directory Services Broker (DSB) está ejecutándose en el cliente NetSEAT. Normalmente, DSB se configura para ejecutarse en el mismo servidor que Policy Director Management Server (IVMgr).

Después de crear una entrada para un Nuevo dominio seguro y de haber pulsado el botón en **Aceptar**, aparecerá el recuadro de diálogo Propiedades del dominio seguro.

1. Pulse el botón en **Añadir**.

   Aparecerá el recuadro de diálogo Adición de un DCE Server.
2. Escriba el nombre de un servidor que proporcione servicios DCE a este dominio seguro.
3. Seleccione uno o más de los siguientes servicios para cada servidor: **Seguridad**, **Hora**, **DSB** o **CDS**.
4. Opcionalmente, puede pulsar el botón en **Avanzadas** si desea definir alguna de las propiedades avanzadas para este DCE Server.

   Consulte el apartado “Definición de las propiedades del DCE Server” en la página 262.
5. Pulse el botón en **Aceptar** para finalizar la definición de los servicios soportados en el DCE Server especificado.

   Volverá a visualizarse el recuadro de diálogo Propiedades del dominio seguro.
6. Acepte los siguientes valores por omisión:
   - Soporte para el inicio de sesión integrado: **Inhabilitado**
   - Inicio de sesión avanzado: **Sólo inicio de sesión DCE**

   Si desea configurar opcionalmente, para el dominio seguro, el soporte de inicio de sesión integrado y el inicio de sesión avanzado, consulte los siguientes apartados:

- Configurar un inicio de sesión integrado (consulte el apartado "Configuración de un inicio de sesión integrado" en la página 265).
- Configurar un inicio de sesión avanzado (consulte el apartado "Configuración del inicio de sesión avanzado (integración PKI)" en la página 268).

7. Cuando acabe de configurar este DCE Server, pulse el botón en **Aceptar**.

   Aparecerá de nuevo la ventana Dominio seguro. Han finalizado las tareas de configuración necesarias para añadir un DCE Server.

Definición de las propiedades del DCE Server

Durante la configuración de un DCE Server, se pueden definir los siguientes valores en el recuadro de diálogo Propiedades avanzadas del DCE Server. Esta tarea de configuración es opcional.

Protocolos y puertas

Para cada DCE Server se puede especificar (opcionalmente) el protocolo (TCP o UDP) que utiliza cada servicio de seguridad. Esta característica puede utilizarse para configurar el funcionamiento a través de cortafuegos como, por ejemplo, IBM SecureWay Firewall Versión 4.1, un componente del producto IBM SecureWay Boundary Server.

Si, por ejemplo, desea deseleccionar el acceso UDP para los servicios de DCE y especificar los números de puertas TCP que ha configurado el administrador de cortafuegos.

Niveles de prioridad

Cuando defina dominios que tengan disponibles varias copias de uno o más servicios, podrá especificar el orden en el que NetSEAT debe acceder a cada servicio. Para asignar su prioridad, puede asignar a cada servicio un número entero positivo. Cuanto más alto sea el número mayor será la prioridad.

Los administradores pueden utilizar esta característica para optimizar el rendimiento al hacer que NetSEAT vaya primero al servicio qué esté más próximo electrónicamente. Si el servicio no está disponible, NetSEAT tomará por omisión la copia del servicio que tenga el siguiente número de prioridad más alto.

1. Para configurar las propiedades avanzadas, vaya al recuadro de diálogo Adición de un DCE Server.
2. Seleccione el **DCE Server**.
3. Pulse el botón en **Avanzadas**.

   Aparecerá el recuadro de diálogo Propiedades avanzadas del DCE Server.
4. Para restringir el protocolo que se utiliza para contactar con un servicio DCE, deseleccione el recuadro de selección que se encuentre junto al servicio DCE adecuado. Al deseleccionar el recuadro de selección, se eliminará el protocolo que no desea tener habilitado.
5. Si es necesario, escriba números de puertas en el campo que se encuentra junto al servicio DCE adecuado.
6. Defina el nivel de prioridad de cada servicio DCE.
7. Pulse el botón en **Aceptar**.

Configuración de NetSEAL Servers

Si desea configurar NetSEAT para que se comunique con un NetSEAL Server, realice los siguientes pasos:

1. Vaya al separador **NetSEAL Servers** y seleccione el dominio seguro desde la lista desplegable.
2. Pulse el botón en **Añadir**.

   Aparecerá el recuadro de diálogo Adición de un NetSEAL Server.
3. Escriba el nombre de la máquina que corresponda al NetSEAL Server.
4. Si NetSEAL utiliza puertas que no sean las puertas por omisión para la tunelización de GSS o SSL, escriba dichos números de puertas en los campos correspondientes. De lo contrario, acepte los valores por omisión.
   - Los protocolos que no se hayan habilitado al crear la entrada del dominio seguro aparecerán en gris.
   - No seleccione el recuadro de selección **Especificar nombre de principal** si está habilitada la tunelización de GSS. Utilice únicamente esta característica para que sea posible la compatibilidad con versiones anteriores.
5. Si está utilizando la tunelización (″tunnel″) de SSL y la configuración de NetSEAT tiene un configurado un servidor proxy SSL, Policy Director seleccionará automáticamente el recuadro de selección **Utilizar servidor proxy**.

   Si no se ha habilitado ningún servidor proxy SSL. el recuadro de selección **Utilizar servidor proxy** está inactivo (deseleccionado y en gris). Para habilitar un servidor proxy SSL en la configuración de NetSEAT, consulte el apartado “Configuración de un proxy SSL” en la página 270.
6. Pulse el botón en **Aceptar**.

   Aparecerá de nuevo el separador **NetSEAL Server**. Ha añadido el NetSEAL Server al la configuración de NetSEAT.

Adición de un servidor protegido

Puede configurar NetSEAT para que especifique un canal de comunicación con servidores de aplicaciones protegidos por un NetSEAL Server.

Se dispone de esta opción cuando el cliente NetSEAT utiliza tunelización (″tunnel) de GSS o de SSL.

Cuando se ha añadido un servidor de aplicaciones a la configuración de NetSEAT, NetSEAT intercepta las peticiones de clientes Windows al servidor de aplicaciones. A continuación, NetSEAT las dirige a un NetSEAL Server a través de un túnel seguro .

Para añadir un servidor protegido a la configuración de NetSEAT, proporcione la siguiente información:

Campo	Definición
Nombre de la máquina	El nombre con el que se denomina al servidor de aplicaciones en el dominio TCP/IP.
Destino del túnel	El nombre del NetSEAL Server que protege al servidor de aplicaciones.
Rango de puertas	El número de la puerta situada en el servidor protegido que esté asegurada por el NetSEAL Server. Esta puerta (o rango de puertas) se especifica en el servidor NetSEAL utilizando el mandato ivadmin.

Protocolo seleccionado	El protocolo de tunelización (″tunnel). Se pueden habilitar ambos protocolos (GSS y SSL) para el dominio seguro. Especifique la tunelización de SSL para Policy Director. La tunelización de GSS se utiliza para conexiones de NetSEAL a NetSEAL.

Para configurar NetSEAT de forma que reconozca las peticiones de salida para un servidor protegido, ejecute estos pasos:

1. Pulse el botón en el separador **Seguridad del sistema principal**.
2. Pulse el botón en **Añadir**.

   Aparecerá el recuadro de diálogo Adición de un servidor protegido.
3. En Nombre de la máquina, escriba el nombre de máquina de un servidor que esté protegido por un NetSEAL Server.

   Un servidor de aplicaciones sólo puede estar protegido por un NetSEAL Server.
4. En Destino del ″tunnel″, utilice la lista desplegable para seleccionar el NetSEAL Server que protege al servidor.
5. Utilice la lista desplegable, si es necesario, para seleccionar el protocolo de tunelización adecuado.
6. Pulse el botón en **Añadir**.

   Aparecerá el recuadro de diálogo Rango de puertas.
7. Especifique la puerta o rango de puertas del NetSEAL Server que NetSEAL utiliza para comunicarse con el servidor de aplicaciones protegido.
8. Pulse el botón en **Aceptar**.

   Aparecerá el recuadro de diálogo Adición de un servidor protegido.

   Por ejemplo, las siguientes entradas en un recuadro de diálogo definen los siguientes valores:
   - Un NetSEAL Server llamado “sol” protege un servidor protegido llamado “trueno.”
   - El servidor sol protege las comunicaciones para trueno en las puertas 5000-5005.
   - Policy Director define un túnel seguro entre el cliente NetSEAT y el NetSEAL Server “sol.”
   - El túnel seguro es del tipo de tunelización (″tunnel″) de SSL.
9. Pulse el botón en **Aceptar**.

   Aparecerá de nuevo el separador **Seguridad del sistema principal**.

   Policy Director añade el servidor protegido a la configuración de NetSEAT.

Adición de una subred protegida

Puede configurar NetSEAT para que especifique un canal de comunicación con una subred protegida por un NetSEAL Server. Se dispone de esta opción cuando el cliente NetSEAT utiliza tunelización (″tunnel) de GSS o de SSL.

Cuando se ha añadido una subred de aplicaciones a la configuración de NetSEAT, NetSEAT intercepta las peticiones de clientes Windows a la subred de aplicaciones. A continuación, NetSEAT las dirige a un NetSEAL Server a través de un túnel seguro .

Para añadir una subred protegida a la configuración de NetSEAT, proporcione la siguiente información:

Campo	Definición
Nombre de cualquier máquina de la subred	El nombre de cualquier servidor de la subred protegida.
Máscara de red	La máscara de red de la subred (por ejemplo, 255.255.0.0).
Destino del ″tunnel″	El nombre del NetSEAL Server que protege la subred.
Seleccionar protocolo	El protocolo de tunelización (″tunnel). Se pueden habilitar ambos protocolos (GSS y SSL) para el dominio seguro. Especifique la tunelización de SSL para Policy Director. La tunelización de GSS se utiliza para conexiones de NetSEAL a NetSEAL.

Para configurar NetSEAT de forma que reconozca las peticiones de salida para una subred protegida por un NetSEAL Server, ejecute estos pasos:

1. Pulse el botón en el separador **Seguridad de la subred**.
2. Seleccione el dominio seguro que contiene el NetSEAL Server que protege la subred.
3. Pulse el botón en **Añadir**.

   Aparecerá el recuadro de diálogo Añadir una subred protegida.
4. Escriba el nombre de cualquier máquina de la subred que esté protegida por el NetSEAL Server.

   Una subred de aplicaciones sólo puede estar protegida por un NetSEAL Server.
5. Entre la máscara de red de la subred.
6. En Destino del ″tunnel″, utilice la lista desplegable para seleccionar el NetSEAL Server que protege la subred.
7. Utilice la lista desplegable, si es necesario, para seleccionar el protocolo de tunelización adecuado.

   Por ejemplo, las siguientes entradas habilitan a NetSEAT para que acceda a una subred con la máscara de red 255.255.0.0. El sistema llamado “trueno” está en la subred. El NetSEAL Server “sol,” que está también en el destino del túnel, protege la subred.

   Nombre de cualquier máquina de la subred: `trueno`

   Máscara de red `255.255.0.0`

   Destino del ″tunnel″ `sol`

   Seleccionar protocolo `SSL`
8. Pulse el botón en **Aceptar**.

   Aparecerá de nuevo el separador **Seguridad de la subred**.

   Policy Director ha configurado el cliente NetSEAT para que se comunique con la subred protegida.

Configuración de un inicio de sesión integrado

Opcionalmente, puede instalar el Soporte de inicio de sesión integrado durante la instalación de NetSEAT. La instalación de NetSEAT cambia el registro de Windows NT para que dé soporte al inicio de sesión integrado.

Después de instalar el inicio de sesión integrado, la herramienta NetSEAT Configuration puede habilitar o inhabilitar el inicio de sesión integrado en cada dominio seguro.

El inicio de sesión integrado puede configurarse durante la instalación y la configuración iniciales de NetSEAT. Si lo prefiere, también puede configurarlo más adelante. La configuración de inicio de sesión integrado se define independientemente para cada dominio seguro.

Antes de configurar el inicio de sesión integrado, un usuario de NetSEAT debe realizar las siguientes tareas:

- Obtener una cuenta en cada dominio seguro en el que sea necesario un inicio de sesión automático.
- Configurar el cliente NetSEAT para que sea miembro de un dominio seguro.
- Sincronizar el nombre de usuario y la contraseña para el inicio de sesión con el dominio seguro con los que se utilizan en el dominio de Windows NT.

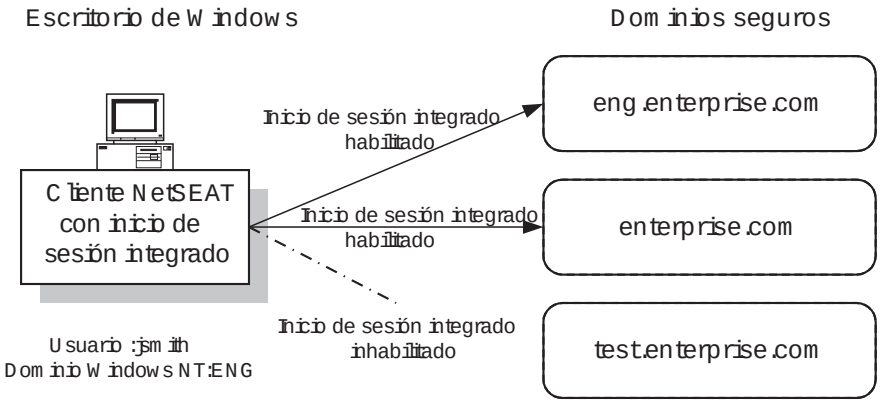
Revisión de un ejemplo de configuración de inicio de sesión integrado

Un técnico llamado John Smith, con el nombre de usuario Windows jsmith, inicia habitualmente la sesión con el dominio de Windows NT ENG. Inicia la sesión con varios dominios seguros, como se indica a continuación:

Nombre del dominio seguro	**Cuenta del usuario del dominio seguro**	**Descripción del dominio seguro**
eng.enterprise.com	jsmith	División técnica del dominio seguro
enterprise.com	ENG/jsmith	El dominio seguro de toda la empresa
test.enterprise.com	test_usuario	Un dominio seguro reducido utilizado únicamente para efectuar pruebas. La célula de test no mantiene un registro completo de nombres de usuarios. Los usuarios inician la sesión como test_usuario.

John Smith utiliza la herramienta de configuración de NetSEAT para configurar el inicio de sesión integrado para cada dominio seguro como se indica a continuación:

Dominio seguro	**Configuración del inicio de sesión integrado**
eng.enterprise.com	Inicio de sesión integrado y configurado para correlacionar al usuario de Microsoft Windows NT jsmith con el usuario del dominio seguro jsmith y para iniciar automáticamente la sesión de jsmith con eng.enterprise.com.
enterprise.com	Inicio de sesión integrado y configurado para correlacionar al usuario de Microsoft Windows NT jsmith con el usuario del dominio seguro ENG/jsmith y para iniciar automáticamente la sesión de ENG/jsmith con enterprise.com.
test.enterprise.com	El inicio de sesión integrado está inhabilitado porque jsmith debe iniciar manualmente la sesión con esta célula como el usuario test_usuario.



Configuración de un inicio de sesión integrado

Para configurar un inicio de sesión integrado:

1. Inicie la herramienta NetSEAT Configuration.

   Aparecerá el separador **Dominios seguros**.
2. Seleccione el dominio seguro para el que desea configurar el inicio de sesión integrado.
3. Pulse el botón en **Editar**.

   Aparecerá la ventana Propiedades del dominio seguro.
4. Seleccione una de las opciones del menú **Soporte para el inicio de sesión integrado**.

   Si **Soporte para el inicio de sesión integrado** aparece en gris, no podrá habilitar el inicio de sesión integrado para este dominio seguro porque no ha instalado el soporte para el inicio de sesión integrado.

   - Seleccione **Inhabilitado** para inhabilitar el soporte para el inicio de sesión integrado en ese dominio seguro.
   - Seleccione **Habilitado—El nombre de usuario DCE es el nombre de usuario Windows** si el nombre de usuario de este dominio seguro coincide con el nombre de usuario Windows.
   - Seleccione **Habilitado—El nombre de usuario DCE es el nombre de dominio Windows/nombre de usuario Windows** si el nombre de usuario de este dominio seguro incluye el nombre del dominio Windows.
5. Pulse el botón en **Aceptar**.

   Aparecerá el separador **Dominios seguros**.
6. Pulse el botón en **Aceptar**.

Configuración de la modalidad de notificación de inicio de sesión integrado

Una contraseña de dominio seguro podría no coincidir con la contraseña del dominio Windows NT. Si no coincide, la entrada del registro Windows determina si los inicios de sesión se ejecutan incorrectamente de forma remota (*modalidad remota*). De lo contrario, solicita al usuario la contraseña actual del dominio seguro *(modalidad interactiva)*. En modalidad remota, Policy Director inicia la sesión del usuario con el dominio de Windows NT, pero no con el dominio seguro. En modalidad interactiva, el usuario puede sincronizar la contraseña del dominio seguro con la contraseña de Windows.

Para cambiar de modalidad de notificación, utilice el editor del registro (Registry Editor) para editar la entrada del registro de Windows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetSEAT\Parameters
```

Modifique el siguiente valor:

```
InfoLevel:
0x00000001 (1)
```

InfoLevel puede tener uno de los siguientes valores:

Valor del registro	Modalidad	Descripción
0	Remota	Después de un intento de inicio de sesión, no se notifican al usuario ni los inicios de sesión correctos ni los incorrectos.
1	Interactiva	Después de un intento de inicio de sesión, se notifican al usuario los inicios de sesión incorrectos y se pide al usuario que lleve a cabo acciones.
2	Verbosa	Después de un intento de inicio de sesión, se notifican al usuario tanto los inicios de sesión correctos como los incorrectos.

Configuración del inicio de sesión avanzado (integración PKI)

Esta tarea de configuración es opcional y se aplica únicamente a clientes NetSEAT que tengan habilitada la tunelización (″tunnel) de GSS.

NetSEAT puede configurarse para integrar un inicio de sesión del usuario con infraestructura de claves públicas (Public Key Infrastructure, PKI) con el inicio de sesión NetSEAT (Kerberos) del usuario.

Por omisión, la integración con el inicio de sesión PKI está inhabilitada. Ejecute la herramienta de configuración de NetSEAT para habilitar el inicio de sesión PKI. El inicio de sesión PKI se habilita o inhabilita separadamente para cada dominio seguro del que participe el cliente NetSEAT.

Releases de PKI soportados

NetSEAT sólo tiene soporte para la integración de un inicio de sesión de usuario con Entrust Versión 4.0.

Nota: El cliente Entrust Versión 4.0 debe instalarse antes de configurar el inicio de sesión PKI de NetSEAT.

Utilización del programa de utilidad de inicio de sesión de NetSEAT

Cuando se llama al programa de utilidad de **inicio de sesión de NetSEAT** desde el menú **Inicio** de Windows, se visualiza un recuadro de selección **Inicio de sesión PKI** al efectuar el inicio de sesión. Este recuadro de selección visualiza los valores de inicio de sesión avanzado configurados para el dominio seguro actual.

Utilización del recuadro de selección de inicio de sesión PKI

Durante el inicio de sesión de NetSEAT, un usuario puede utilizar el recuadro de selección **Inicio de sesión PKI** para alterar temporalmente la configuración de inicio de sesión de PKI para un inicio de sesión. La alteración temporal resulta útil si se había seleccionado el valor **Inicio de sesión PKI con retroceso a inicio de**

sesión de DCE durante la configuración. Los usuarios pueden alterar temporalmente la configuración si desean eludir el intento de inicio de sesión PKI y efectuar un inicio de sesión con DCE. En ese caso, el usuario debe deseleccionar el recuadro de selección **Inicio de sesión PKI** para forzar un inicio de sesión con DCE.

Si, durante la configuración, un usuario había configurado **Sólo inicio de sesión PKI**, el deseleccionar el recuadro de selección **Inicio de sesión PKI** durante el inicio de sesión no surte efecto.

Si, durante la configuración, un usuario había configurado **Sólo inicio de sesión DCE**, la selección del recuadro de selección **Inicio de sesión PKI** durante el inicio de sesión produce un mensaje de error.

Utilización del inicio de sesión de la bandeja del sistema

Para efectuar un inicio de sesión NetSEAT puede utilizar el icono **NetSEAT** de la Bandeja del sistema. Utilice la lista desplegable para seleccionar el dominio con el que desea efectuar el inicio de sesión. Si se ha configurado el inicio de sesión PKI, aparecerá el indicador de inicio de sesión de Entrust.

Si el inicio de sesión PKI no se ejecuta correctamente y ha configurado **Inicio de sesión PKI con retroceso a inicio de sesión de DCE**, Policy Director solicitará que se realice un inicio de sesión de DCE.

Configuración de inicio de sesión avanzado

Para integrar un inicio se sesión PKI con el inicio de sesión NetSEAT:

1. Inicie la herramienta NetSEAT Configuration.

   Aparecerá el separador **Dominios seguros**.
2. Seleccione el dominio seguro para el que desea configurar el inicio de sesión PKI.
3. Pulse el botón en **Editar**.

   Aparecerá el recuadro de diálogo Nuevo dominio seguro.
4. Pulse el botón en **Configurar**.

   Aparecerá la ventana Propiedades del dominio seguro.
5. En el área de Inicio de sesión avanzado, seleccione una de las opciones de inicio de sesión avanzado de la lista desplegable.
   - Seleccione **Sólo inicio de sesión DCE** para que el usuario pueda iniciar la sesión con el dominio seguro de Policy Director utilizando un nombre de usuario y una contraseña (inicio de sesión Kerberos).
   - Seleccione **Inicio de sesión PKI con retroceso a inicio de sesión de DCE** para que el usuario pueda intentar un inicio de sesión PKI. Si el inicio de sesión no es correcto, NetSEAT pedirá al usuario que entre un nombre de usuario y una contraseña para un inicio de sesión DCE.
   - Seleccione **Sólo inicio de sesión PKI** para pedir al usuario que inicie la sesión utilizando un certificado X.509.
6. Pulse el botón en **Aceptar**.

   Aparecerá el recuadro de diálogo Nuevo dominio seguro.
7. Pulse el botón en **Aceptar**.

   Aparecerá el separador **Dominios seguros**.

Definición del delta de tiempo máximo

Esta tarea de configuración es opcional y se aplica únicamente a clientes NetSEAT de Policy Director Management Console y a servidores de Windows NT para Policy Director.

NetSEAT utiliza servicios remotos de tiempo cuando está configurado para utilizar la tunelización (″tunnel″) de GSS. Puede configurar el delta de tiempo máximo permitido entre la hora del dominio seguro y el reloj del sistema NetSEAT. También puede utilizar el valor por omisión (15 minutos).

Para definir el delta de tiempo máximo:

1. Pulse el botón en el separador **General**.
2. Si es necesario, escriba un valor en el campo **Delta de tiempo máximo**.
3. Pulse el botón en **Aceptar** o en **Aplicar**.

Denegación de acceso a los recursos de red

Esta tarea de configuración es opcional y se aplica únicamente a clientes NetSEAT que tengan habilitada la tunelización (″tunnel) de GSS o SSL.

Puede impedir a los usuarios efectuar peticiones inseguras a TELNET, RLOGIN o HTTP desde una estación de trabajo. Configure el cliente NetSEAT para que deniegue o limite el acceso a estos servicios de red. La denegación o limitación de acceso obliga a la estación de trabajo a utilizar únicamente canales de comunicaciones Policy Director seguros y cifrados al iniciar conversaciones por la red.

Por omisión, esta función está desactivada. Esta característica sólo debería activarse para redes altamente seguras con finalidades especiales.

Para denegar el acceso a servicios de red no protegidos:

1. Seleccione el separador **General**.
2. Si lo desea, seleccione el recuadro de selección **Denegación de acceso a servicios de la red no protegidos**.
3. Pulse el botón en **Aceptar** o en **Aplicar**.

Configuración de un proxy SSL

Esta tarea de configuración es opcional y se aplica únicamente a clientes NetSEAT que tengan habilitada la tunelización (″tunnel) de SSL.

Cuando las peticiones procedentes del cliente NetSEAT deben ir a través de un servidor proxy SSL de la red, puede configurar NetSEAT para que utilice el servidor proxy. En el separador **General**, el recuadro de selección **Habilitar servidor proxy** habilita el servidor proxy para que puedan utilizarlo todos los NetSEAL Servers.

Si deselecciona este recuadro de selección, ninguno de los NetSEAL Servers que se hayan añadido a la configuración de NetSEAT podrá acceder al servidor proxy.

Para especificar un servidor proxy SSL, lleve a cabo los siguientes pasos:

1. Pulse el botón en el separador **General.**

2. Si es necesario, cambie el número de minutos que aparece en el campo **Delta de tiempo máximo**. El valor por omisión es de 15 minutos.
3. Asegúrese de no haber seleccionado el recuadro de selección **Denegación de acceso a servicios de la red no protegidos**.
4. Seleccione el recuadro de selección **Habilitar servidor proxy**.
5. Escriba el nombre pertinente en el campo **Nombre de la máquina servidor proxy.**
6. Entre el número de la puerta en el campo **Puerta del servidor proxy**.
7. Pulse el botón en **Aceptar** o en **Aplicar**.

Utilización de los programas de utilidad de seguridad de NetSEAT

El cliente NetSEAT facilita los programas de utilidad de seguridad de DCE que se encuentran en las implementaciones tradicionales de DCE. La arquitectura exclusiva de NetSEAT permite ampliar las funciones estándar de cada uno de estos programas de utilidad: **klist**, **kdestroy** y **dce_login**.

klist

El mandato **klist** lista el usuario primario (*principal*) y los elementos retenidos en la antememoria de credenciales por omisión. Si utiliza la opción **-c**, este mandato listará el usuario y los elementos contenidos en la antememoria que identifica el nombre de la antememoria.

NetSEAT ejecuta las opciones estándar del mandato **klist** y añade otras opciones.

Las opciones estándar son las siguientes:

Opción	Descripción
-c *nombre antememoria*	Indica que debe visualizarse el contenido de la antememoria identificada por el nombre de antememoria en vez del contenido de la antememoria por omisión.
-e	Incluye elementos caducados en la visualización. Sin esta opción, sólo se visualizan los elementos actuales.
-f	Visualiza valores de opciones de los elementos.

Las opciones añadidas son las siguientes:

Opción	Descripción
-C *nombre célula*	Describe el usuario primario y los elementos mantenidos para el usuario en la célula DCE identificada por *nombre célula.*
-m	Describe el usuario primario y los elementos mantenidos para el usuario en todas las células DCE para las cuales el usuario tiene un contexto de inicio de sesión DCE.
-s	Visualizar un corto resumen de todas las células con las que el usuario ha iniciado la sesión y el nombre de inicio de sesión del usuario para cada una de las células.

kdestroy

El mandato **kdestroy** destruye el contexto de inicio de sesión de un usuario y las credenciales de dicho usuario. Hasta que Policy Director restablece las credenciales, el usuario y todos los procesos creados por el usuario sólo pueden realizar accesos no autentificados.

El cliente NetSEAT tiene soporte para la opción estándar **kdestroy** y añade otras opciones.

La opción estándar es:

Opción	Descripción
-c *nombre antememoria*	Indica el contexto de inicio de sesión y las credenciales asociadas al nombre de la antememoria deben destruirse en vez de las que se encuentran en la antememoria por omisión.

Las opciones añadidas son las siguientes:

Opción	Descripción
-C *nombre célula*	Destruye el contexto de inicio de sesión y las credenciales asociadas de la célula especificada en *nombre célula*.
-m	Destruye el contexto de inicio de sesión del usuario y las credenciales asociadas de todas las células en las que el usuario tiene un contexto de inicio de sesión.

dce_login

El mandato **dce_login** valida la identidad de un usuario, obtiene las credenciales de red del usuario y establece un contexto de inicio de sesión DCE.

El usuario debe suministrar un nombre_principal (nombre de usuario) y una contraseña. Si no facilita estos valores como argumentos de línea de mandatos, **dce_login** se los pedirá.

El cliente NetSEAT tiene soporte para las siguientes opciones estándar de **dce_login**:

Opción	Descripción
-exec *serie-mandatos*	Ejecuta el mandato especificado por la *serie_mandatos* tras el inicio de sesión. Si la *serie_mandatos* se especifica sin un nombre completo de vía de acceso, el prefijo de la vía de acceso se obtiene buscando en los directorios según lo indicado por la variable PATH.
-k *nombre_archivo_claves*	Indica a **dce_login** que obtenga un nombre de usuario (principal) y una contraseña del archivo de claves *nombre_archivo_claves*.
-r	Renueva el contexto de inicio de sesión DCE del usuario antes de que caduque el elemento del usuario.

Policy Director tiene soporte para la siguiente opción de dce_login añadida:

Opción	Descripción
-C *nombre célula*	Especifica un inicio de sesión de usuario con la célula *nombrecélula* en vez de iniciar la sesión con la célula por omisión.

Nota: El cliente NetSEAT no tiene soporte para la opción **dce_login -c**.

Resolución de problemas con netseat_ping

El cliente NetSEAT proporciona el programa de utilidad **netseat_ping** que permite habilitar a un usuario para que obtenga información sobre el estado de los servicios DCE en una o más células. Utilice **netseat_ping** para determinar si los siguientes servicios están disponibles:

- Security Services
- Time Services
- Cell Directory Services
- Directory Services Broker

Para saber el estado de los servicios de todas las células con las que el usuario mantiene un contexto de inicio de sesión, escriba:

```
netseat_ping
```

Por ejemplo, si configura un cliente NetSEAT para que participe de la célula redback aparecerá 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[ ] is available (v3.0)
                    ncacn_ip_udp:redback[ ] is available (v3.0)
```

Policy Director tiene soporte para las siguientes opciones de **netseat_ping**:

Opción	Descripción
-C *nombre célula*	Genera una lista de enlaces para todos los servidores configurados por el usuario para la célula *nombre célula*.
-t -C *nombre célula*	Visualiza los enlaces con Time Server en la célula *nombre célula*.
-s -C *nombre célula*	Visualiza los enlaces con Security Server en la *nombre célula*.
-c -C *nombre célula*	Visualiza los enlaces con el servidor CDS en la célula *nombre célula*.
-d -C *nombre célula*	Visualiza los enlaces con el servidor DSB en la célula *nombre célula*.

Si hay más de un Security Server, Time Server, Cell Directory Server o DSB en la célula, **netseat_ping** intentará sondearlos todos.

Capítulo 21. NetSEAT: Directory Services Broker

Este capítulo proporciona una visión general de Directory Services Broker (DSB) y explica cómo personalizar la configuración de DSB para el entorno del usuario.

Este capítulo incluye los siguientes temas:

Visión general de Directory Services Broker

El cliente NetSEAT de Policy Director descarga la funcionalidad de la interfaz RPC Name Service Interface en Directory Services Broker (DSB). El DSB actúa como servidor Cell Directory Services (CDS) de la gama media.

El cliente NetSEAT dirige al DSB las peticiones de ubicación de recursos y servicios. El DSB, a su vez, se pone en contacto con CDS para resolver la petición. A continuación, el DSB devuelve la información solicitada al sistema que ejecuta el cliente NetSEAT.

Policy Director instala y configura automáticamente el DSB durante la instalación de Policy Director. Policy Director proporciona el producto DSB como parte del paquete del Management Server (IVMgr). No es necesario efectuar ninguna otra operación para utilizar un DSB.

- Los clientes NetSEAT, que sirven como módulo de soporte de Policy Director Servers y de Management Console, utilizarán el DSB.
- Los clientes NetSEAT que utilizan la tunelización de SSL no utilizan el DSB.

El DSB puede soportar un gran número de clientes NetSEAT. Para dominios seguros más grandes, puede optimizar el rendimiento ejecutando el DSB en un servidor que proporcione Cell Directory Services.

Para facilitar una alta disponibilidad o para equilibrar la carga en redes muy grandes, un administrador puede considerar conveniente utilizar más un DSB en un dominio seguro. Puede instalar y configurar manualmente DSB adicionales.

Opciones de configuración de Directory Services Broker

DSB se ejecuta como daemon o como servicio. El DSB puede iniciarse automáticamente al rearrancar el sistema. En la mayoría de las situaciones, el DSB no requiere administración.

Las siguientes secciones explican cómo puede ajustar un administrador los parámetros de configuración de DSB:

Definición de la puerta de DSB

El DSB está a la escucha de peticiones en una puerta. Por omisión, el DSB elige una puerta al azar.

Opcionalmente, un administrador puede especificar el número de puerta entrando un valor en uno de los siguientes archivos:

UNIX: /etc/services

Windows: *vía-instalación*\system32\drivers\etc\services

Por ejemplo, para indicar a un DSB de un sistema UNIX que escuche en la puerta 5000, coloque la siguiente entrada en /etc/services:

```
dsb                5000/tcp              # Directory
Services Broker
```

Especificación de la ubicación del archivo de anotaciones cronológicas de DSB

El DSB utiliza archivos de anotaciones cronológicas de servicios DCE para anotar cronológicamente notificaciones, errores, avisos y errores irrecuperables (muy graves). Si su instalación DCE utiliza servicios DCE, DSB grabará la salida en uno o más archivos de anotaciones cronológicas de servicios. Los archivos de anotaciones cronológicas de DCE se encuentran en el directorio *DCELOCAL*/var/svc. *DCELOCAL* es el directorio de instalación de DCE.

Puede haber varios archivos que reflejen el estado de un mensaje como, por ejemplo, una notificación, un error o un aviso. Puede especificar la ubicación de esos archivos colocando entradas en el archivo de rutas *DCELOCAL*/var/svc/routing.

Por ejemplo:

```
NOTICE:FILE:DCELOCAL/var/svc/notice
```

También puede especificar esa ubicación utilizando la variable de entorno *SVC_NOTICE*. La definición de la variable de entorno altera temporalmente la especificación del archivo de rutas. Por ejemplo, podría definir una variable de entorno UNIX para la especificación de un archivo de notificaciones, como sigue:

```
export SVC_NOTICE=FILE:DCELOCAL/var/svc/notice
```

Ejemplo de línea de mandatos:

Si define NOTICE en un archivo de rutas e inicia el DSB desde una línea de mandatos, como se indica a continuación:

```
SVC_NOTICE=FILE:DCELOCAL/var/dsb/dsb.log dsb -q -f -U cell_admin -P *****
```

El DSB realizará las siguientes tareas:

- Se configurará e iniciará a si mismo de forma remota.
- Anotará cronológicamente todas las notificaciones en *DCELOCAL*/var/dsb/dsb.log.
- Anotará cronológicamente todos los errores, avisos y errores irrecuperables (muy graves) según lo especificado en el archivo de rutas.
- No visualizará ninguna salida del registro cronológico.

Si desea ver la información completa sobre el formato de archivos de rutas y la utilización del grupo SVC_* de variables de entorno, consulte la información sobre servicios de DCE. Encontrará la siguiente documentación para la instalación y configuración de DCE en el CD IBM Policy Director Security Services, en el directorio /doc:

- DCE22_QuickBeginnings_AIX.pdf
- DCE22_QuickBeginnings_NT.pdf
- DCE20_InstallGuide_Solaris.pdf
- DCE20_ReleaseNotes_Solaris.pdf

Opciones de línea de mandatos de Directory Services Broker

En la siguiente tabla se describen las opciones de línea de mandatos de DSB:

Opción	Descripción
-d	Se ejecuta en segundo plano, en vez de en un daemon UNIX o un servicio Microsoft Windows NT. Esta opción se utiliza primordialmente para la depuración.
-f	Fuerza la reconfiguración de las entradas de seguridad DCE de DSB. Este indicador crea el grupo Director/dsb-servers de Policy Director (a menos que ya se haya creado), el archivo de tabla de tecleo y el principal (usuario) *nombre_completo_DNS*, donde *nombre_completo_DNS* es el sistema en el que se ejecuta DSB. Esta opción se utiliza en el arranque inicial de DSB. Puede llamarse más de una vez sin necesidad de eliminar primero la entrada del principal (usuario), la entrada de grupo ni los archivos de la tabla de tecleo.
-h	Mensaje de uso de la línea de mandatos.
-q	Envía salida estándar a un archivo de anotaciones cronológicas en vez de enviarla a stdout o stderr. No se enviará ninguna notificación a la pantalla.
-r	Desconfigura el DSB. Esta opción suprime las entradas de seguridad DCE del DSB (como se explica arriba en la opción **-f**). El indicador **-r** se utiliza solo o con **-q**. No puede utilizarse ningún otro indicador línea de mandatos con **-r**.
-t	Especifica el número de hebras que utilizará el servidor. El número de hebras define el número de peticiones de clientes que pueden procesarse simultáneamente.
-P *contraseña*	Especifica la contraseña para el inicio de sesión DCE del principal (usuario). Se utiliza únicamente con el indicador **-U**.
-U *nombre_principal*	El inicio de sesión DCE del principal (usuario) utilizado para ejecutar la configuración del DSB. Utilice esta opción para indicar cualquier usuario que tenga delegada la autorización para crear las entradas de seguridad de DSB (como se explica arriba en opción **-f**).

-b	*Sólo Microsoft Windows*—Especifica el nombre de archivo del binario ejecutable del DSB. Utilice esta opción si el DSB se ha instalado en una ubicación que no sea la ubicación por omisión. Esta opción almacena la ubicación del DSB en el registro de Microsoft Windows NT. Microsoft Windows NT utiliza el valor del registro cuando se configura el DSB como servicio de Microsoft Windows NT.
-v	*Sólo Microsoft Windows*—Visualiza la versión del DSB y el mensaje del proveedor de DCE.

Apéndice A. Administración de Policy Director utilizando ivadmin

El programa de utilidad **ivadmin** es una línea de mandatos equivalente a la de Management Console que puede utilizarse para realizar tareas de administración.

Este capítulo incluye los siguientes temas:

Presentación del programa de utilidad ivadmin

El programa de utilidad **ivadmin** es una alternativa a la línea de mandatos de Management Console. Los administradores que deseen automatizar determinadas funciones de gestión podrá hacerlo escribiendo scripts que utilicen **ivadmin**.

Muchos de los mandatos de **ivadmin** duplican funciones que ya proporciona Management Console. Pero además, **ivadmin** facilita varias funciones avanzadas de gestión que no están disponibles con Management Console. El paquete IVBase que se instala en cualquier sistema que ejecute Policy Director instala también este programa de utilidad de forma parte del mismo paquete.

Inicio del programa de utilidad ivadmin

Para iniciar el programa de utilidad **ivadmin**, inicie la sesión con un dominio seguro utilizando **dce_login**. A continuación, escriba:

UNIX: `# ivadmin`

Windows: `ivadmin`

Aparecerá el indicador **ivadmin**:

```
ivadmin>
```

Escriba en el indicador los mandatos, opciones y argumentos adecuados. Consulte las tablas de mandatos del apartado "Utilización de los mandatos de ivadmin" en la página 280.

Por ejemplo, para ver los mensajes de ayuda de **ivadmin**, escriba:

```
ivadmin> help
```

Salida del programa de utilidad ivadmin

Para salir del programa de utilidad y volver al indicador de mandatos, escriba el mandato **ivadmin exit**:

```
ivadmin> exit
```

Utilización de los mandatos de ivadmin

Los mandatos de **ivadmin** son los siguientes:

Nota: Todos los mandatos de **ivadmin** deben entrarse en una línea como un solo mandato. Algunos de los ejemplos utilizados en este manual son largos y, para mostrarlos, continúan en la línea siguiente.

Mandatos de servidor (server)

Los mandatos **ivadmin server** proporcionan funciones que actualmente no facilita Management Console:

Mandato	Descripción
server flush_logs *nombre-servidor*	
	Graba los archivos de anotaciones cronológicas de WebSEAL Server de la memoria en el disco duro. Permite un seguimiento inmediato de los sucesos del servidor.
server list	
	Lista todos los servidores configurados.
server resume *nombre-servidor*	
	Reanuda un WebSEAL Server suspendido.
server show *nombre-servidor*	
	Visualiza las propiedades del servidor especificado como, por ejemplo, su nombre, descripción, nombre de sistema principal y URL root.
server start *nombre-servidor*	
	Inicia el servidor especificado. Inicia secmgrd (NetSEAL y WebSEAL) e ivacld.
server stop *nombre-servidor*	
	Detiene el servidor especificado. Detiene secmgrd (NetSEAL y WebSEAL) e ivacld.
server suspend *nombre-servidor*	
	Suspende el WebSEAL Server especificado. Resulta útil para efectuar el mantenimiento del servidor.

Los siguientes mandatos **ivadmin server** amplían la funcionalidad de Management Console:

Mandato	Descripción

server delete /ExternAuthzn/*nombre-servidor*	
	Elimina únicamente un servidor de autorizaciones externo. Normalmente, este mandato lo utiliza de forma no interactiva un programa de desinstalación. **Nota**: Este mandato no debe utilizarse para suprimir ningún otro servidor.
server modify *nombre-servidor* **baseurl** *punto-montaje*	
	Especifica la rama del espacio de ACL que utilizará el servidor. Se utiliza con WebSEAL Servers reproducidos. Indica que el *punto-montaje* de la rama especificada será la rama maestra que utilizará Management Console para la administración de ACL. Las ACL de la rama se aplicarán a todos los servidores reproducidos conectados con Smart Junction a este punto de montaje (punto de conexión Smart Junction); los servidores reproducidos reflejan inmediatamente todos los cambios en las ACL. Tenga en cuenta que el *punto-montaje* se refiere al objeto contenedor /WebSEAL y debe encontrarse en el directorio WebSEAL (no en alguno de los subdirectorios).
server register externauth *nombre-servidor ubicación-en principal-servidor car-acción nombre-acción*	
	Registra la existencia de un servidor de autorizaciones externo. Utilice este mandato para informar a Policy Director Authorization Service de que existe un servidor de autorizaciones externo que debe consultarse para resolver privilegios de autorización en objetos protegidos.
server status *servidor de estado*	
	Indica si el servidor está funcionando o se ha detenido y si la réplica de la base de datos se ha actualizado con los cambios más recientes.

Notas técnicas:

Para visualizar las propiedades del WebSEAL Server en la máquina `chevelle`, escriba:

```
ivadmin> server show /WebSEAL/chevelle
Tipo: WebSEAL Server
Nombre: /WebSEAL/chevelle
Descripción: chevelle
Nombre del sistema principal: chevelle
Ubicación de NS: /.:/subsys/intraverse/secmgr/server/chevelle
Principal: secmgr/chevelle Root URL: /chevelle
```

Tenga en cuenta que debe escribir el argumento *nombre-servidor* con el formato exacto visualizado en la salida del mandato **ivadmin server list**.

Por ejemplo:

```
ivadmin> server list
         /WebSEAL/chevelle
         /NetSEAL/chevelle
         /ExternAuthzn/timechecker
```

Mandatos de objetos (object)

Los siguientes mandatos **ivadmin object** proporcionan las mismas funciones que los mandatos equivalentes de tareas de gestión del espacio de objetos (Object Space) de Management Console:

Mandato	Descripción

object list *nombre-directorio*	
	Lista los objetos agrupados bajo el directorio indicado y visualiza el nombre de las ACL asociadas a cada objeto. Tenga en cuenta que este mandato no amplía el árbol más allá del directorio.
object show *nombre-objeto*	
	Visualiza la información correspondiente al *nombre-objeto* y el nombre de las ACL que pueda tener asociadas. Si no hay ninguna ACL asociada, aparecerá la frase `No ACL`.

Mandatos de acción (action)

Utilice los siguientes mandatos **ivadmin action** para definir acciones adicionales de autorización (permisos) de Policy Director en Management Console.

Por ejemplo, utilice los mandatos **ivadmin action** para añadir un mecanismo de autorización externo a la lista de permisos de ACL disponibles.

Los mandatos **ivadmin action** proporcionan funciones que actualmente no facilita Management Console:

Mandato	**Descripción**
action create *nombre descripción tipo-acción*	
	Define una nueva acción de autorización (permiso) de Policy Director. Crea un nuevo código de permiso de ACL que representa dicha acción en Management Console. El argumento *nombre* indica el nuevo código de permiso de una sola letra. El argumento *descripción* proporciona la etiqueta del nuevo recuadro de selección que aparecerá en Management Console. El argumento *tipo-acción* proporciona una etiqueta para la categoría de acción tal como se visualiza en Management Console. Ejemplo: `ivadmin> action create k time Ext-Authzn`
action delete *nombre*	
	Elimina una acción de autorización (permiso) existente creada mediante el mandato **action create**. Ejemplo: `ivadmin> action delete k`
action list	

	Lista todas las acciones de ACL (permisos) existentes con el siguiente formato:
	nombre permiso descripción permiso tipo acción
	
	Ejemplo:
	`ivadmin> action list`
	
	Visualizaría una información parecida a ésta:
	`r read WebSEAL`
	`...`

Mandatos de ACL (acl)

Los siguientes mandatos **ivadmin acl** proporcionan las mismas funciones que los mandatos equivalentes de tareas de gestión **ACL** de Management Console:

Mandato	Descripción
acl attach *nombre-objeto nombre-acl*	
	Une una plantilla de ACL a un objeto.
acl create *nombre-acl*	
	Crea una nueva plantilla de ACL en la base de datos de plantillas de ACL. Tenga en cuenta que este mandato no crea entradas de ACL.
acl delete *nombre-acl*	
	Elimina una plantilla de ACL de la base de datos de plantillas de ACL.
acl detach *nombre-objeto*	
	Deshace la unión de la plantilla de ACL actual con el objeto indicado. Tenga en cuenta que este mandato no elimina la plantilla de ACL de la base de datos de plantillas de ACL.
acl find *nombre-acl*	
	Busca y lista todos los objetos que tenga unida la plantilla de ACL indicada.
acl list	
	Lista todas las plantillas de ACL de la base de datos de plantillas de ACL.
acl modify *nombre-acl* **descripción** *desc*	
	Permite crear o editar el campo de descripción asociado a la plantilla de ACL indicada. Uno de los lugares donde aparece esta descripción es en el área de Definición de ACL del panel de tarea de gestión de ACL de Management Console.
acl modify *nombre-acl* **remove user** *nombre-usuario*	
	Permite suprimir una entrada de ACL de un usuario existente de la definición de plantilla de ACL indicada.
acl modify *nombre-acl* **remove group** *nombre-grupo*	
	Permite suprimir una entrada de ACL de un grupo existente de la definición de plantilla de ACL indicada.
acl modify *nombre-acl* **remove any-other**	
	Permite eliminar la entrada de ACL autentificada por cualquiera de la definición de plantilla de ACL indicada.
acl modify *nombre-acl* **remove unauthenticated**	
	Permite eliminar la entrada de ACL no autentificada de la definición de plantilla de ACL indicada.
acl modify *nombre-acl* **set user** *nombre-usuario perms*	
	Permite crear o editar la entrada de ACL de un usuario (`pubs`) en la definición de plantilla de ACL indicada, en la que los permisos (*perms*) son `bPTr`. Ejemplo: `ivadmin> acl modify pubs set user pedro bPTr`
acl modify *nombre-acl* **set group** *nombre-grupo perms*	

	Permite crear o editar la entrada de ACL de un grupo en la definición de plantilla de ACL indicada. Ejemplo: `ivadmin> acl modify pubs set group ventas Tr`
acl modify *nombre-acl* **set any-other** *perms*	
	Permite crear o editar la entrada de ACL (pubs) autentificada por cualquiera en la definición de plantilla de ACL indicada. Ejemplo: `ivadmin> acl modify pubs set any-other r`
acl modify *nombre-acl* **set unauthenticated** *perms*	
	Permite crear o editar la entrada de ACL no autentificada de la definición de plantilla de ACL indicada. Ejemplo: `ivadmin> acl modify pubs set unauthenticated r`
acl show *nombre-acl*	
	Lista el conjunto completo de entrada que forman la definición de la plantilla de ACL indicada. `ivadmin> acl show pubs`

Mandatos de NetSEAL

Utilizando el programa de utilidad **ivadmin** podrá ejecutar las siguientes tareas de administración de NetSEAL:

- "Gestión de redes protegidas".
- "Gestión de conexiones Smart Junction de NetSEAL" en la página 285.
- "Gestión de puertas protegidas" en la página 285.
- "Gestión de alias de puertas protegidas" en la página 286.

Gestión de redes protegidas

Se puede pensar en las *redes* como si fuesen servidores no Policy Director protegidos por NetSEAL. Utilice los mandatos de **ivadmin netseal** para añadir, suprimir y listar redes protegidas.

Mandato	**Descripción**
netseal network add *red máscara-red* **[***alias-red***]**	
	Crea una nueva red que debe proteger NetSEAL. El par red / máscara de red son números de dirección estándar de red IP y máscaras de red. El nombre de alias de red opcional puede utilizarse para identificar la red. Si no se especifica ningún alias, la red debe identificarse mediante el par de red y máscara de red. Se recibirán errores si la red ya existe.
netseal network delete *id-red*	
	Elimina del sistema la red especificada, donde *id-red* puede corresponder a uno de los siguientes elementos: • par *red/máscara de red* • *alias de red* Se recibirá un error si la red no se encuentra dentro de la base de datos.
netseal network list	

	Visualiza todas las redes de la base de datos, lo que incluye el par de red y máscara de red así como todos los alias definidos.

Gestión de conexiones Smart Junction de NetSEAL

Las conexiones Smart Junction de NetSEAL determinan en qué dirección debe ir la comunicación a través de un Policy Director Server. Pueden crearse conexiones Smart Junction entre dos Policy Director Servers o entre un Policy Director Server y una red. Utilice un túnel GSS para asegurar la comunicación a través de una conexión Smart Junction entre dos Policy Director Servers.

Utilice los mandatos de **ivadmin netseal junction** para añadir, eliminar y listar conexiones Smart Junction de NetSEAL.

Mandato	**Descripción**
netseal junction add *nombre-sist-pral destino*	
	Crea una conexión (junction) de un NetSEAL Server a un destino especificado en el que *nombre sistema principal* es el nombre del NetSEAL Server menos el nombre del dominio, y *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Se reciben errores si la conexión (junction) ya existe, el servidor del sistema principal no existe o el destino no existe.
netseal junction delete *nombre-sist-pral* **destino**	
	Elimina la conexión (junction) de un NetSEAL Server con el destino especificado, siendo *nombre sistema principal* el nombre del NetSEAL Server menos el nombre de dominio; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Se recibe un error si la conexión Smart Junction no existe. El mandato no tiene ningún efecto en las conexiones actuales.
netseal junction list *nombre sistema principal*	
	Visualiza todas las conexiones Smart Junction de NetSEAL para el NetSEAL Server especificado.

Gestión de puertas protegidas

Policy Director NetSEAL Server proporciona servicios de seguridad para puertas, sistemas principales y redes específicos. Por ejemplo, NetSEAL Server puede configurarse para asegurar el tráfico de TELNET en una puerta determinada.

Utilice los mandatos de **ivadmin netseal port** para añadir, eliminar y listar puertas protegidas. Puede especificar puertas para servidores o redes Policy Director.

Mandato	**Descripción**
netseal port add *destino id-puerta*	

	Protege conexiones con el destino especificado en el ID-puerta indicado, donde *destino* puede corresponder a uno de los siguiente elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Donde *id-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* • *alias de puerta* Se recibe un error si la puerta ya está protegida, si el servidor no existe o el alias de puerta no existe.
netseal port delete *destino id-puerta*	
	Detiene la protección de conexiones con el destino especificado en la puerta especificada; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Donde *id-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* • *alias de puerta* Se recibe un error si la puerta no está protegida aún, si el servidor no existe o el alias de puerta no existe.
netseal port list *destino*	
	Visualiza una lista de todas las puertas del destino especificado; *destino* puede corresponder a uno de los siguientes elementos: • *servidor-pd* • par *red/máscara de red* • *alias de red* Se recibe un error si el servidor no existe.

Nota: El **rango de puertas** debe expresarse como dos números de puerta separados por un guión (por ejemplo: 22-88).

Gestión de alias de puertas protegidas

Utilice los mandatos de **ivadmin port-alias** para añadir, eliminar y listar alias de puertas. Utilice los *alias de puertas* para identificar rangos de puertas detectados de una forma que tenga más sentido.

Mandato	**Descripción**
netseal port-alias add *espec-puerta alias-puerta*	
	Crea un nuevo alias de puerta para la puerta especificada; *espec-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* Recibirá un error si el rango de puertas ya tiene otro alias.
netseal port-alias delete *id-puerta*	

	Elimina del sistema el id-puerta especificado; *id-puerta* puede corresponder a uno de los siguientes elementos: • *puerta* • *rango de puertas* • *alias de puerta* El *id-puerta* puede corresponder a una puerta, un rango de puertas o un nombre de alias de puerta. Se recibirá un error si el alias de puerta no se encuentra dentro de la base de datos.
netseal port-alias list	
	Visualiza todos los alias de puerta que se encuentran dentro de la base de datos.

Mandatos de gestión de configuración

Los mandatos de gestión de configuración **ivadmin admin** visualizan información sobre el servidor.

Mandato	Descripción
admin show configuration	

	Visualiza información que indica si el registro de usuario se encuentra en LDAP o DCE.
	
	Ejemplo:
	`ivadmin> admin show configuration`
	
	Produciría una salida parecida a ésta:
	`LDAP:`
	`TRUE`
	`SECAUTHORITY: Default`
	`GSO: TRUE`

Mandatos de gestión de usuarios

Los siguientes mandatos **ivadmin user** proporcionan las mismas funciones que los mandatos de tareas de gestión de **Usuarios** equivalentes de Management Console. Este conjunto de mandatos controla las entradas de usuarios en el registro LDAP por omisión.

Un *usuario* es un usuario de Policy Director. Un *usuario GSO* es un usuario de Policy Director que tiene además autorización para trabajar con recursos de la Web como, por ejemplo, un servidor Web.

Mandato	Descripción
user create [-gsouser] ***nombre-usuario dn cn sn contr***	

	Crea una nueva cuenta de usuario (secUser) de Policy Director en el registro de usuarios LDAP cuyo nombre distinguido no existe aún en la base de datos de registros LDAP por omisión. El argumento **-usuariogso** es opcional. El guión (-) es necesario en los mandatos opcionales. Cuando se especifica el argumento -usuariogso, el usuario se convierte también en un usuario de GSO (usuariogso). El argumento *nombre-usuario* es el nombre del usuario que va a crearse. Este nombre debe ser exclusivo. El argumento *dn* indica el nombre distinguido de LDAP asignado al usuario que va a crearse (por ejemplo, `cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US`). El DN debe ser exclusivo. El argumento *cn* es el nombre común asignado al usuario que va a crearse (por ejemplo, `Diana Lucas`). El argumento *sn* es el apodo del usuario que va a crearse (por ejemplo, `Lucas`). El argumento *contr* es la contraseña definida para el nuevo usuario. Las contraseñas deben cumplir con las políticas de contraseñas establecidas por el administrador de Policy Director (por ejemplo, `micontraseña`). Ejemplo: `ivadmin> user create -gsouser dlucas cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US "Diana Lucas" Lucas micontraseña` Para que la cuenta de usuario sea válida, deberá activar manualmente el usuario modificando la información sobre el mismo. Para modificar la información, debe dar al indicador account-valid (cuenta válida) el valor “yes” (sí). Para añadir una descripción del usuario, deberá utilizar el mandato **ivadmin modify user** a fin de modificar la información sobre la cuenta del usuario.
user import [-gsouser] ***nombre-usuario***	
	Permite que un usuario existente cuyo nombre distinguido ya exista en la base de datos de registros LDAP por omisión se actualice con información de Policy Director de forma que el usuario pueda participar del dominio seguro. Ejemplo: `ivadmin> user import -gsouser mlucaser cn=Mike Lucaser,ou=Austin,o=Wesley Inc,c=US`
user modify ***nombre-usuario*** **descripción** *descripción*	
	Añade una descripción que proporciona al administrador información que le facilita la identificación del usuario. Ejemplo: `ivadmin> user modify dlucas Descripción "Diana Lucas, Credit Dept HCUS`
user modify ***nombre-usuario*** **password** *contraseña*	

	Cambia la contraseña actual del usuario por otra distinta. No será necesario confirmar la contraseña. Ejemplo: `ivadmin> user modify dlucas password` *`nuevacontraseña`*
user modify *nombre-usuario* authentication-mechanism *mecanismo*	
	Cambia el mecanismo utilizado para la autentificación. Ejemplo: `ivadmin> user modify dlucas authentication-mechanism dce`
user modify *nombre-usuario* account-valid {yes | no}	
	Indica si una cuenta está activa o inactiva. Para activar la cuenta, seleccione “yes” (sí); para desactivar la cuenta, seleccione “no.” Ejemplo: `ivadmin> user modify dlucas account-valid yes`
user modify *nombre-usuario* password-valid {yes | no}	
	Indica si una contraseña está activa o inactiva. Para activar la contraseña, seleccione “yes” (sí); para desactivar la contraseña, seleccione “no.” Ejemplo: `ivadmin> user modify dlucas password-valid no`
user modify *nombre-usuario* gsouser {yes | no}	
	Indica si el usuario de Policy Director especificado es también un usuario GSO. Para añadir el usuario como usuario GSO, seleccione “yes” (sí); para que el usuario deje de ser un usuario GSO, seleccione “no.” Ejemplo: `ivadmin> user modify dlucas gsouser no`
user delete *nombre-usuario*	
	Elimina una cuenta de usuario existente del registro de usuarios LDAP. Cuando se elimina una cuenta de usuario Policy Director se suprime también la información de la cuenta del usuario del registro LDAP por omisión. Ejemplo: `ivadmin> user delete dlucas` Automáticamente, todas las credenciales de recursos asociadas a la cuenta del usuario se eliminan al mismo tiempo que la cuenta del usuario.
user show *nombre-usuario*	
	Visualiza información sobre la cuenta del usuario especificado. Ejemplo: `ivadmin> user show dlucas`
user show-dn *dn*	

	Proporciona información adicional sobre el usuario cuando se especifica el nombre distinguido (DN).
	
	Ejemplo:
	`ivadmin> user show-dn`
	`cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US`

user show-groups ***nombre-usuario***	

	Visualiza los grupos a los que pertenece el usuario especificado.
	
	Ejemplo:
	`ivadmin> user show-groups dlucas`
	
	Produciría una lista parecida a ésta:
	`ventas`
	`crédito`
	`técnico`

user list ***patrón máx-devol***	

	Genera una lista de todas las cuentas de usuarios configurados, listada por nombres de usuario, que corresponda al patrón especificado. La lista visualiza los usuarios en el orden en que se crearon las cuentas de usuario.
	
	El argumento *patrón* permite especificar un patrón indicando lo que se desea listar. El comodín busca coincidencias en los nombres de usuarios. El patrón puede incluir una combinación de comodines y constantes de cadenas de caracteres y es sensible a las mayúsculas y minúsculas (por ejemplo, `*luca*`).
	
	El argumento *máx-devol* limita la cantidad de entradas que se encontrarán y devolverán en una sola petición (por ejemplo, 2). Est número también depende de la configuración del servidor LDAP, donde puede especificarse el número máximo de resultados que puede devolverse como parte de una operación de búsqueda. Policy Director devuelve el valor que sea más pequeño entre *máx-devol* y el valor configurado en el servidor LDAP.
	
	Ejemplo:
	`ivadmin> user list *luca* 2`
	
	Produciría una lista parecida a ésta:
	`dlucas`
	`mlucaser`

user list-dn ***patrón máx-devol***	

	Si tan solo se conoce una parte del nombre distinguido, genera una lista de todas las cuentas de usuario configuradas, listadas por nombre distinguido. La lista visualiza los usuarios en el orden en que se crearon los nombres de usuario.
	
	El comodín compara la parte correspondiente al CN del nombre distinguido del usuario, excluyendo la parte del cn=.
	
	El número *máx-devol* también depende de la configuración del servidor LDAP, donde puede especificarse el número máximo de resultados que puede devolverse como parte de una operación de búsqueda. Policy Director devuelve el valor que sea más pequeño entre *máx-devol* y el valor configurado en el servidor LDAP.
	
	Ejemplo:
	`ivadmin> user list-dn *luca* 2`
	
	Produciría una lista parecida a ésta:
	`Diana Lucas,ou=Austin,o=Wesley Inc,c=US`
	`Mike Lucaser,ou=Austin,o=Wesley Inc,c=US`

Notas técnicas:

Tenga en cuenta que debe entrar el argumento *dn* del mandato **user show-dn** y del mandato **user show-groups-dn** con el formato exacto que se visualiza en el mandato group show dn. Use comillas dobles (″) cuando el argumento *dn* contenga espacios.

Por ejemplo:

```
cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US
```

Los mandatos **user show** y **user show-dn** visualizarían información parecida a la siguientes para el usuario Diana Lucas:

```
ID de inicio de sesión: dlucas
LDAP dn: cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US
LDAP cn: Diana Lucas
LDAP sn: Lucas
Descripción: Diana Lucas, Credit Dept HCUS
ES SecUser: true
Es usuario de GSO: false
Cuenta válida: true
Contraseña válida: true
Mecanismo de autorización:
Valor por omisión: LDAP
```

Mandatos de gestión de grupo

Los siguientes mandatos **ivadmin group** son el equivalente de los mandatos de tareas de gestión de **Grupos** de Management Console. Este conjunto de mandatos de gestión controla las entradas de grupos en el registro de directorios de LDAP.

Un *grupo* es un conjunto de cuentas de Policy Director que tiene atributos similares. Los grupos permiten a un administrador utilizar un nombre de grupo en una lista de control de accesos (ACL) en vez de indicar cada usuario individualmente.

Podrá eliminar o cambiar todas las entradas de grupos que desee. Además, podrá visualizar información sobre los miembros de uno o varios grupos. Como administrador, también podrá listar todos los grupos configurados:

Mandato	Descripción
group create ***nombregrupo dn cn***	
	Crea un nuevo grupo de Policy Director (SecGroup) en el registro de usuarios de LDAP. El argumento *nombregrupo* es el nombre del grupo que va a crearse. Este nombre debe ser exclusivo. El argumento *dn* indica el nombre distinguido de LDAP asignado al grupo que va a crearse (por ejemplo, `cn=credit Lucas,ou=Austin,o=Wesley Inc,c=US`). El argumento *cn* es el nombre común asignado al grupo (por ejemplo, `Credit Lucas`). Ejemplo: `ivadmin> group create credit cn=credit,ou=Austin,o=Wesley Inc,c=US Credit`
group import ***nombregrupo***	
	Importa la información sobre un grupo existente en el registro LDAP para crear un grupo de Policy Director. El grupo ya debe existir en el registro LDAP para que un grupo de Policy Director pueda importar la información y crear el grupo. El nombre del grupo que va a crearse debe ser exclusivo. Ejemplo: `ivadmin> group import engineering cn=engineering,ou=Austin,o=Wesley Inc,c=US`
group modify ***nombregrupo*** **description** *descripción*	
	Añade una descripción al grupo especificado para que el administrador de Policy Director pueda identificarlo más fácilmente. Ejemplo: `ivadmin> group modify credit description "Credit, Dept HCUS`
group modify ***nombregrupo*** **add** *nombre-usuario*	
	Añade un nuevo usuario al grupo especificado. Ejemplo: `ivadmin> group modify engineering add dlucas`
group modify ***nombregrupo*** **remove** *nombre-usuario*	
	Elimina un usuario existente del grupo especificado. Ejemplo: `ivadmin> group modify engineering remove dlucas`
group delete ***nombregrupo***	
	Elimina un grupo existente y todas las entradas asociadas al grupo. Ejemplo: `ivadmin> group delete engineering`
group show ***nombregrupo***	

	Visualiza los detalles de un grupo especificado. Ejemplo: `ivadmin> group show credit`
group show-dn *dn*	
	Proporciona el nombre del grupo al que pertenece el nombre distinguido especificado. Ejemplo: `ivadmin> group show-dn cn=credit,ou=Austin,o=Wesley Inc,c=US`
group show-members *nombregrupo*	

	Visualiza los miembros del grupo especificado, listados por nombre distinguido.
	
	Ejemplo:
	`ivadmin> group show-members credit`
	
	Visualizaría una información parecida a ésta:
	`dlucas`
	`mlucaser`

group list *patrón máx-devol*	

	Genera una lista de todos los grupos configurados, cuyos nombres coincidan con el patrón especificado, listados por nombre de grupo.
	
	El argumento *patrón* permite especificar un patrón indicando lo que se desea listar. El comodín busca coincidencias en los nombres de grupos. El patrón puede incluir una combinación de comodines y constantes de cadenas de caracteres y es sensible a las mayúsculas y minúsculas (por ejemplo, `*Austin*`).
	
	El argumento *máx-devol* limita la cantidad de entradas que se encontrarán y devolverán en una sola petición (por ejemplo, 2). Est número también depende de la configuración del servidor LDAP, donde puede especificarse el número máximo de resultados que puede devolverse como parte de una operación de búsqueda. Policy Director devuelve el valor que sea más pequeño entre *máx-devol* y el valor configurado en el servidor LDAP.
	
	Visualizaría una información parecida a ésta:
	`crédito`
	`marketing`

group list-dn *patrón máx-devol*	

	Si tan solo se conoce una parte del nombre distinguido, genera una lista de todos los grupos configurados, listados por nombre distinguido y correspondientes al patrón especificado.
	
	El comodín compara la parte correspondiente al CN del nombre distinguido del grupo, excluyendo la parte del cn=.
	
	El número *máx-devol* también depende de la configuración del servidor LDAP, donde puede especificarse el número máximo de resultados que puede devolverse como parte de una operación de búsqueda. Policy Director devuelve el valor que sea más pequeño entre *máx-devol* y el valor configurado en el servidor LDAP.
	
	Ejemplo:
	`ivadmin> group list-dn *t* 2`
	
	Visualizaría una información parecida a ésta:
	`cn=credit,ou=Austin,o=Wesley Inc,c=US`
	`cn=marketing,ou=Boston,o=Austin Sale,c=US marketing`

Notas técnicas:

Tenga en cuenta que debe entrar el argumento *dn* con el formato exacto que se visualiza en la salida del mandato **group show-dn**. Use comillas dobles (″) cuando el argumento *dn* contenga un espacio.

Por ejemplo:

```
cn=credit,ou=Austin,o=Wesley Inc,c=US
```

Los mandatos **group show** y **group show-dn** visualizan información parecida a la siguientes para el grupo credit:

```
ID de grupo: credit
LDAP dn: cn=credit,ou=Austin,o=Wesley Inc,c=US
Descripción: Credit, Dept HCUS
LDAP cn: credit
Es SecGroup: true
```

Mandatos de gestión de recursos

Los siguientes mandatos **ivadmin** de Policy Director son un conjunto de mandatos de gestión que controlan la información relacionada con recursos.

La información relacionada con recursos se explica en los siguientes apartados:

- “Gestión de recursos”
- “Gestión de grupos de recursos” en la página 295
- “Gestión de credenciales de recursos” en la página 297

Gestión de recursos

Los siguientes mandatos **ivadmin rsrc** permiten al administrador gestionar distintos recursos, como, por ejemplo los servidores Web para usuarios de GSO.

Un *recurso* es un servidor Web. El identificador **-T** de una definición Smart Junction identifica el servidor Web.

Un mandato **ivadmin rsrc** identifica el nombre del recurso de la Web.

Los siguientes mandatos **ivadmin rsrc** proporcionan las mismas funciones que los mandatos equivalentes de gestión de tareas de **Recursos GSO** de Management

Console.

Mandato	Descripción
rsrc create *nombre-recurso* [-desc *descripción*]	
	Crea y denomina un servidor Web como recurso. El argumento *nombre-recurso* es el nombre que se le ha dado al recurso de la Web para identificarlo (por ejemplo, `engwebs01`). El argumento *descripción* es una descripción opcional que puede añadirse para que el administrador de Policy Director identifique más fácilmente el recurso. Todos los parámetros opcionales deben ir precedidos de un guión (-). Las descripciones que contengan algún espacio en blanco deben estar entre comillas dobles (″). `ivadmin> rsrc create engwebs01 -desc "Engineering Web server - Room 4807"`
rsrc delete *nombre-recurso*	
	Elimina el recurso nombrado, incluida la información de descripción. El recurso debe existir, de lo contrario se visualizará un error. Ejemplo: `ivadmin> rsrc delete engwebs01`
rsrc list	

	Visualiza los nombres de todos los recursos de la web definidos en el directorio LDAP, listados por nombre de recurso.
	
	Ejemplo:
	
	`ivadmin> rsrc list`
	
	Visualizaría una información parecida a ésta:
	
	`engwebs01`
	`engwebs02`
	`engwebs03`

rsrc show *nombre-recurso*	

	Visualiza la información del recurso de la Web para el recurso nombrado.
	
	El recurso debe existir, de lo contrario se visualizará un error.
	
	Ejemplo:
	
	`ivadmin> rsrc show engwebs01`
	
	Visualizaría una información parecida a ésta:
	
	`Nombre de recurso de la Web: engwebs01`
	`Descripción: Engineering Web server - Room 4807`

Gestión de grupos de recursos

Los siguientes mandatos **ivadmin rsrcgroup** son equivalentes a los mandatos de las tareas de gestión de **Grupos de recursos GSO** que controlan la información de Recursos GSO. Estos mandatos permiten al administrador gestionar distintos atributos relacionados con grupos de recursos.

Un *grupo de recursos* indica un grupo de servidores Web en el que todos los servidores del grupo tienen los mismos conjuntos de ID de usuario y de contraseña. Se puede crear una sola credencial de recurso para todos los recursos

del grupo de recursos. Policy Director utiliza una sola credencial de recurso para un grupo de recursos en vez de crear una credencial de recurso para cada recurso del grupo de recursos.

Los siguientes mandatos **ivadmin rsrcgroup** proporcionan las mismas funciones que los mandatos equivalentes de gestión de tareas de **Grupos de recursos GSO** de Management Console.

Mandato	**Descripción**
rsrcgroup create *nombre-grupo-recursos* [-desc *descripción*]	
	Crea y denomina un grupo de recursos de la Web. El argumento *nombre-grupo-recursos* es el nombre del grupo de recursos. El argumento *descripción* es una descripción opcional que puede añadirse para identificar al grupo de recursos. Los parámetros opcionales **-desc** deben ir precedidos de un guión (-). Las descripciones que tengan algún espacio en blanco deberán estar entre comillas dobles. Ejemplo: `ivadmin> rsrcgroup create webs4807 -desc "Web servers, Room 4807"`
rsrcgroup delete *nombre-grupo-recursos*	
	Elimina el grupo de recursos nombrado, incluida la información de descripción. El grupo de recursos debe existir. Ejemplo: `ivadmin> rsrcgroup delete webs4807`
rsrcgroup modify *nombre-grupo-recursos* add rsrcname *nombre-recurso*	
	Añade un recurso de la Web a un grupo de recursos existente. El grupo de recursos debe existir. Ejemplo: `ivadmin> rsrcgroup modify webs4807 add rsrcname engwebs02`
rsrcgroup modify *nombre-grupo-recursos* remove rsrcname *nombre-recurso*	
	Elimina un nombre de recurso de la Web de un grupo de recursos existente. Ejemplo: `ivadmin> rsrcgroup modify webs4807 remove rsrcname engwebs02`
rsrcgroup list	

	Visualiza los nombres de todos los grupos de recursos de la Web definidos en el directorio LDAP. La información que aparece después de “list” se ignora.
	
	Ejemplo:
	`ivadmin> rsrcgroup list`
	
	Visualizaría una información parecida a ésta:
	`webs4807`
	`websbld3`
	`websbld4`

rsrcgroup show *nombre-grupo-recursos*	

	Visualiza la información del recurso de la Web para el grupo de recursos nombrado.
	
	El grupo de recursos debe existir, de lo contrario se visualizará un error.
	
	Ejemplo:
	`ivadmin> rsrcgroup show webs4807`
	
	Visualizaría una información parecida a ésta:
	`Nombre`
	`de grupo de recursos: webs4807`
	`Descripción: Web servers, Room 4807`
	`Miembros del recurso:`
	`engwebs01`
	`engwebs02`
	`engwebs03`

Gestión de credenciales de recursos

Los siguientes mandatos **ivadmin rsrccred** permiten al administrador gestionar distintos atributos relacionados con credenciales de recursos.

Una *credencial de recurso* proporciona una identificación y una contraseña de usuario para un recurso GSO específico del usuario como, por ejemplo, un servidor Web o un grupo de servidores Web.

"web" o "group" sólo pueden especificarse como grupos de recursos cuando se utilizan los mandatos **ivadmin rsrccred**.

Nota: Para poder aplicar los mandatos de credenciales de recursos, el recurso o el grupo de recursos ya deben existir.

Mandato	**Descripción**
rsrccred create *nombre-recurso* **rsrcuser** *idusuario-recurso* **rsrcpwd** *contraseña-recurso* **rsrctype {web | group} user** *nombre-usuario*	

	Crea una credencial de recurso y le da nombre. El usuario y el recurso (o el grupo de recursos) ya deben existir para poder crear la credencial de recurso. Si el usuario, recurso o grupo de recursos no existen o no se han especificado, se visualizará un mensaje de error. Los tipos de recursos sólo incluyen recursos “web” o “group” cuando se trata de mandatos de gestión de credenciales de recursos. El argumento *nombre-recurso* es el nombre que se le ha dado al recurso al crearlo (por ejemplo, `engwebs01`). El argumento *idusuario-recurso* es la identificación exclusiva del usuario (ID de usuario) en el servidor Web (por ejemplo, `4807ws01`. El argumento *contraseña-recurso* es la contraseña de un usuario en el servidor Web (por ejemplo, *rsrcpwd*). El argumento *nombre-usuario* es el nombre del usuario al que se aplica la información de credencial de recurso(por ejemplo, `dlucas`). Ejemplo: `ivadmin> rsrccred create engwebs01 rsrcuser 4807ws01 rsrcpwd rsrcpwd rsrctype web user dlucas`
rsrccred modify *nombre-recurso* rsrctype {web | group} set [-rsrcuser *idusuario-recurso*] [-rsrcpwd *contraseña-recurso*] user *nombre-usuario*	
	Cambia la información de ID de usuario y de contraseña de la credencial de recurso del recurso especificado. Para cambiar o restablecer la información de ID de usuario o de contraseña del recurso, estos mandato opcionales deben ir precedidos de un guión (-). Para poder cambiar la información de credencial del recurso, es necesario que el recurso o grupo de recursos y el usuario ya existan. El tipo de recurso especificado debe coincidir con el tipo de recurso que se le asignó al crearlo (por ejemplo, “web” o “group”). Ejemplo: `ivadmin> rsrccred modify engwebs01 rsrctype group set -rsrcuser 4807ws01 -rsrcpwd newrsrpw user dlucas`
rsrccred delete *nombre-recurso* rsrctype {web | group} user *nombre-usuario*	
	Elimina únicamente la información de credencial de recurso de un usuario existente. El tipo de recurso debe coincidir con el tipo de recurso que se le asignó al crearlo (por ejemplo, “web” o “group”). Ejemplo: `ivadmin> rsrccred delete engwebs01 rsrctype group user dlucas`
rsrccred list user *nombre-usuario*	

	Visualiza los nombres y tipos de todos los recursos definidos para el usuario especificado.
	
	Ejemplo:
	`ivadmin> rsrccred list user dlucas`
	
	Visualizaría una información parecida a ésta:
	`Nombre de recurso: engwebs01`
	`  Tipo de recurso: group`
	`Nombre de recurso: engwebs02`
	`  Tipo de recurso: web`

rsrccred show *nombre-recurso* rsrctype {web | group} user *nombre-usuario*	

	Visualiza la información de credencial de recurso de un usuario especificado.
	
	La credencial de recurso y el usuario deben existir ya, de contrario se visualizará un mensaje de error.
	
	Ejemplo:
	`ivadmin> rsrccred show webs4807 rsrctype group user dlucas`
	
	Visualizaría una información parecida a ésta:
	`Nombre de recurso: engwebs01`
	`  Tipo de recurso: group`
	`ID de usuario de recurso: dlucas`

Mandatos de gestión de políticas del registro

Los mandatos **ivadmin policy** son un conjunto de mandatos de gestión que controlan la información general sobre políticas para usuarios de Policy Director. El administrador puede gestionar los siguientes atributos de políticas:

- "Gestión de políticas de inicio de sesión".
- "Gestión de políticas de contraseña" en la página 300

Una política (*policy*) define el conjunto de limitaciones impuestas a cuentas y contraseñas para mejorar la seguridad global del sistema. Estas limitaciones puede imponerse generalmente (globalmente a todos los usuarios del sistema) o específicamente (sólo a un usuario especificado). Si se ha aplicado una política específica a un usuario, dicha política específica tendrá prioridad sobre cualquier otra política general que también pueda haberse definido. La prioridad se aplica independientemente de si la política especificada es más o menos restrictiva que la política general.

Gestión de políticas de inicio de sesión

Los siguientes mandatos **ivadmin policy** permiten al administrador gestionar políticas relacionadas con el inicio de sesión.

Utilice los mandatos **policy** de tareas de gestión relacionadas con el inicio de sesión para crear nuevas políticas de inicio de sesión o copias las políticas existentes. También podrá visualizar información sobre la política de inicio de sesión de una cuenta de usuario.

Para políticas relacionadas con el inicio de sesión, Policy Director define el tiempo relativo como DDD-hh:mm:ss, y define el tiempo absoluto como AAAA-MM-DD-hh:mm:ss cuando se refiere a mandatos **policy** de tareas de gestión.

Mandato	Descripción
policy {set | get} max-account-age [*tiempo-relativo*] [-user *nombre-usuario*]	

	Gestiona la política que controla el período de tiempo, como número máximo de días y horas, que falta para que caduque la cuenta que pertenece al usuario.
	
	Ejemplos:
	`ivadmin> policy set max-account-age 031-12:30:00 dlucas`
	
	O:
	`ivadmin> policy get max-account-age dlucas`

policy {set | get} account-expiry-date [*tiempo-absoluto*] [-user *nombre-usuario*]	

	Especifica la fecha y hora absolutas en que caduca la cuenta de un usuario determinado. También puede utilizarse para especificar cuándo van a caducar simultáneamente todas las cuentas de usuarios.
	
	Ejemplos:
	`ivadmin> policy set account-expiry-date 1999-12-30-23:30:00 dlucas`
	
	O:
	`ivadmin> policy get account-expiry-date dlucas`

Gestión de políticas de contraseña

Los siguientes mandatos **ivadmin policy** permiten al administrados gestionar distintos atributos de políticas relacionadas con la contraseña.

Para políticas relacionadas con las contraseñas, Policy Director define el tiempo relativo como DDD-hh:mm:ss cuando se refiere a mandatos **policy** de tareas de gestión.

Mandato	Descripción
policy {set | get} min-password-length [*número*]	

	Especifica la longitud mínima, en caracteres, de una contraseña. El argumento *número* indica la longitud mínima autorizada para una contraseña.
	
	Ejemplos:
	`ivadmin> policy set min-password-length 8`
	
	O:
	`ivadmin> policy get min-password-length`

Apéndice B. 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 Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
Estados Unidos

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 se facilita únicamente con fines de planificación. Puede estar sujeta a cambios antes de que los productos descritos estén disponibles.

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.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente que ilustran técnicas de programación en distintas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo en la forma que desee y sin necesidad de abonar ninguna cantidad a IBM, para el desarrollo, utilización, comercialización o distribución de programas de aplicación que se ajusten a la interfaz de programas de aplicación para la que se han escrito los programas.

Estos ejemplos no se han probado exhaustivamente en todas las condiciones. Por lo tanto,IBM no puede garantizar (ni implicar) la fiabilidad, posibilidad de servicios ni funcionalidad de estos programas. Puede copiar, modificar y distribuir estos programas de ejemplo en la forma que desee y sin necesidad de abonar ninguna cantidad a IBM, para el desarrollo, utilización, comercialización o distribución de programas de aplicación que se ajusten a la interfaz de programas de aplicación de IBM.

Las copias de la totalidad o parte de estos programas de ejemplo o cualquier trabajo que se derive de los mismos, debe incluir una nota de copyright como se indica a continuación:

© (el nombre de su empresa) (año). Parte de este código procede de IBM Corp. Programas de ejemplo. © Copyright IBM Corp. *indique el o los años.* Reservados todos los derechos.

Si está visualizando esta información en copia software, es posible que no aparezcan las fotografías ni las ilustraciones en color.

Marcas registradas

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

AIX
DCE
IBM
FirstSecure
Global Sign-On
GSO
LDAP
Policy Director
SecureWay

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de terceros.

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
IntraVerse	DASCOM, Inc.
Internet Information Server (IIS)	Microsoft Corporation

Internet Explorer	Microsoft Corporation
Netscape y logotipos de Netscape	Netscape Communications Corporation
Logotipos de Netscape	Netscape Communications Corporation
Netscape FastTrack	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Smart Junctions	DASCOM, Inc.
Solaris	Sun Microsystems, Inc
WebSEAL	DASCOM, Inc.

Java y todas las marcas registradas basadas 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

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Glosario

Este glosario define los términos y abreviaturas de este manual que son nuevos o pueden no resultar familiares, así como los términos que pueden resultar de interés. Incluye términos y definiciones procedentes de:

- IBM Dictionary of Computing, New York: McGraw-Hill, 1994.
- American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1998.

A

ACL. Lista de control de accesos.

algoritmo de firma digital. Algoritmo de clave pública que se utiliza como parte del estándar de firma pública (Digital Signature Standard). No puede utilizarse para el cifrado sino únicamente para firmas digitales.

American National Standard Code for Information Interchange (ASCII) (Código Nacional Americano de Normas para el Intercambio de Información). El código de normas que se utiliza para el intercambio de información entre sistemas de proceso de datos, sistemas de comunicación de datos y el equipo asociado. El conjunto ASCII utiliza un juego de caracteres codificado formado por caracteres de 7 bits codificados (8 bits incluido un bit para el control de paridad). El juego de caracteres consta de caracteres de control y caracteres gráficos.

American National Standards Institute (ANSI) (Instituto Nacional Americano de Normas). Organismo que establece los procedimientos mediante los cuales los organismos acreditados crean y mantienen normas voluntarias para la industria en los Estados Unidos. Está formado por productores, consumidores y grupos de interés general.

anotación cronológica de auditoría. Tabla de una base de datos que almacena un registro por suceso de auditoría.

ANSI. American National Standards Institute.

API. Interfaz de programas de aplicación.

aplicación Java. Programa autónomo escrito en lenguaje Java. Se ejecuta fuera del contexto de un navegador Web.

applet. Programa informático escrito en Java y que se ejecuta dentro de un navegador web compatible con Java. Conocido también como applet Java.

applet Java. *Vea* applet. *Compare con*aplicación Java.

ASCII. American National Standard Code for Information Interchange (Código Nacional Americano de Normas para el Intercambio de Información).

autentificación. Proceso en el que se determina de forma fiable la identidad de una parte de la comunicación.

autentificación de usuario. Proceso en el que se valida que el emisor de un mensaje es el propietario identificable y autorizado del mensaje. Valida también el hecho que el usuario se esté comunicando con el usuario final o sistema que se deseaba.

autoridad de certificación (CA). El software responsable de seguir las políticas de seguridad de una empresa y de asignar identidades electrónicas seguras en forma de certificados. La CA puede procesar peticiones de autoridades de registro (Registration Authorities, RA) pare emitir, renovar y revocar certificados. La CA interactúa con la RA del producto IBM SecureWay Trust Authority para publicar certificados y CRL en el Directorio. *Vea también* certificado digital.

autoridad de registro (RA). Software de IBM SecureWay Trust Authority que administra certificados digitales para asegurar la aplicación de las políticas comerciales de una empresa desde la recepción inicial de una petición inscripción hasta la revocación del certificado.

autorización. Permiso para acceder a un recurso.

B

base de datos de registros. Contiene información sobre peticiones de certificados y certificados emitidos. La base de datos almacena datos de inscripciones y todas las modificaciones en los datos de los certificados mientras existen.

biblioteca de almacenamiento de datos. Módulo que proporciona acceso a almacenamientos de datos permanentes de certificados, CRL, claves, políticas y demás objetos relacionados con la seguridad.

C

CA. Autoridad de certificación.

CAS. Credentials Acquisition Service.

CA superior. La CA que se encuentra en la parte superior de una jerarquía de CA de PKI.

certificación. Proceso durante el cual un tercero fiable emite una credencial electrónica que responde de la identidad de un individuo, empresa u organismo.

certificación cruzada. Modelo de fiabilidad en que una CA emite para otra CA un certificado que contiene la clave pública asociada a su clave de signatura privada. Un certificado cruzado permite a los sistemas clientes o entidades finales de un dominio administrativo comunicarse de forma segura con sistemas clientes o entidades finales de otro dominio.

certificación digital. *Vea* certificación.

certificado de navegador. Certificado digital conocido también como certificado del área del cliente. Lo emite una CA a través de un servidor Web habilitado por SSL. La claves de un archivo cifrado permiten al poseedor del certificado cifrar, descifrar y firmar datos. Normalmente, es el navegador Web quien almacena las claves. Algunas aplicaciones permiten el almacenamiento de las claves en tarjetas inteligentes u otros soportes. *Vea también* certificado digital

certificado de servidor. Certificado digital, emitido por una CA para habilitar a un servidor Web para que dirija transacciones basadas en SSL. Cuando un navegador se conecta con el servidor utilizando el protocolo SSL, el servidor envía al navegador su clave pública. Esto permite la autentificación de la identidad del servidor. También permite el envío de información cifrada al servidor. *Vea también*certificado de CA, certificado digital, *y*certificados de navegador.

certificado de ubicación. Parecido a un certificado CA, pero sólo válido para una ubicación especifica de la Web. *Vea también*certificado de CA

certificado digital. Credencial electrónica que emite un tercero fiable para una persona o entidad. Cada certificado está firmado con la clave privada de la CA. Responde de la identidad de un individuo, empresa u organización.

Dependiendo de la función de la CA, el certificado puede dar fe de la autoridad del portador para realizar e-business a través de Internet. En cierro sentido, un certificado digital tiene una función similar a la de un permiso de conducción o un diploma médico. Certifica que el portador de la clave privada correspondiente está autorizado a realizar determinadas actividades de e-business.

Un certificado contiene información sobre la entidad que certifica, tanto si es una persona como una máquina o un programa informático. Incluye la clave pública certificada de la entidad.

certificados de CA. Certificado que el navegador Web acepta, cuando se le solicita, de una CA que no reconoce. El navegador puede utilizar entonces el certificado para autentificar las comunicaciones con servidores que contienen certificados emitidos por dicha CA.

certificado X.509. Estándar de certificación ampliamente aceptado, diseñado para dar soporte a una gestión y distribución seguras de certificados firmados digitalmente a través de redes de Internet seguras. El certificado X.509 define las estructuras de datos que contienen procedimientos para la distribución de claves públicas firmadas digitalmente por terceros fiables.

certificado X.509 Versión 3. El certificado X.509v3 tiene estructuras de datos ampliadas para almacenar y recuperar información de aplicación de certificados, información de distribución de certificados, información de revocación de certificados, información de políticas y firmas digitales.

Los procesos de X.509v3 crear CRL con indicación de la hora para todos los certificados. Cada vez que se utiliza un certificado, las posibilidades de X.509v3 permiten a la aplicación comprobar la validez del certificado. También permiten que la aplicación determine si el certificado se encuentra en la CRL. Pueden crearse CRL de X.509v3 con un periodo de validez específico. También pueden basarse en otras circunstancias que pueden invalidar el certificado. Por ejemplo, si un empleado deja una empresa, su certificado se colocaría en la CRL.

CGI. Common Gateway Interface.

cifrado. En la seguridad informática, los principios, medios y métodos para cifrar texto plano y descifrar texto cifrado.

cifrado/descifrado. Utilizando la clave pública del futuro receptor, cifrar datos para dicha persona que, a continuación, utilizará la clave privada del par para descifrar los datos.

cifrar. Transformar datos con el fin de ocultar su significado.

cifrar. Mezclar información de forma que solamente alguien que tenga el código de descifrado adecuado pueda obtener la información original mediante el descifrado.

clase. En el diseño o programación orientados a objetos, grupo de objetos que comparten una definición común y, por lo tanto, comparten también propiedades, operaciones y comportamientos comunes.

clave. Cantidad utilizada en el cifrado para cifrar o descifrar información.

clave de cifrado de documento. Normalmente, una clave de cifrado/descifrado simétrico, como, por ejemplo, DES.

clave privada. La clave de un par de claves pública/privada de la que sólo puede disponer su propietario. Permite al propietario recibir una transacción privada o efectuar una firma digital. Los datos firmados con un clave privada sólo pueden verificarse con la clave pública privada. *Compare con* clave pública.*Vea también* par de claves pública/privada.

clave pública. La clave de un par de claves pública/privada que está a disposición de terceros. Les permite dirigir una transacción al propietario de la clave o verificar una firma digital. Los datos cifrados con la clave pública sólo pueden descifrarse con la clave correspondiente. *Compare con* clave privada. *Vea también* par de claves pública/privada.

cliente. (1) Unidad funcional que recibe servicios compartidos de un servidor. (2) Un sistema o programa que solicita un servicio a otro sistema o programa.

cliente/servidor. En un proceso distribuido, modelo en el que un programa situado en una ubicación envía una petición a un programa de otra ubicación y espera una respuesta. El programa que efectúa la solicitud se denomina cliente; el que responde se denomina servidor.

codificación base64. Medio común de transmisión de datos binarios con MIME.

Common Cryptographic Architecture (CCA). Software de IBM que permite un planteamiento coherente con el cifrado en las principales plataformas informáticas de IBM. Tiene soporte para software de aplicaciones escrito en varios lenguajes de programación. El software de aplicaciones puede llamar a los servicios CCA para ejecutar una amplia gama de funciones de cifrado como, entre otras, los cifrados de DES y RSA.

Common Gateway Interface (CGI). Método estándar para transmitir información entre páginas Web y servidores Web.

comprobación de integridad. Comprobación de los registros de auditoría que sean el resultado de transacciones con componentes externos.

confidencialidad. Propiedad de no divulgación a partes no autorizadas.

cortafuego. Barrera entre redes que limita el flujo de información entre redes. Normalmente, la finalidad de un cortafuego es proteger las redes internas contra el uso no autorizado desde el exterior.

credencial. Información confidencial utilizada para probar una identidad en un intercambio de autentificación. En entornos informáticos de red, el tipo más común de credencial es un certificado creado y firmado por una CA.

Credentials Acquisition Service (CAS). El componente Credentials Acquisition Service (CAS) de Policy Director.

CRL. Lista de revocación de certificados.

D

daemon. Programa que lleva a cabo tareas en segundo plano. Se le llama implícitamente cuando se produce una condición que requiere su ayuda. No es necesario que los usuarios tengan constancia de un daemon puesto que, normalmente, el sistema lo activan automáticamente. Un daemon puede estar para siempre en el sistema o el sistema puede tener que regenerarlo a intervalos.

Este término inglés procede de la mitología. Posteriormente, se adaptó su sentido al que acrónimo de Disk And Execution MONitor (DAEMON).

Data Encryption Standard (DES). Codificación de cifrado de bloques, definida y adoptada por el gobierno de EE. UU. en 1977 como estándar oficial. Originalmente desarrollado por IBM. DES se ha estudiado ampliamente desde su publicación y es un sistema de cifrado bien conocido y muy utilizado.

DES es un sistema de cifrado simétrico. Cuando se utiliza para comunicaciones, tanto el emisor como el receptor deben conocer la misma clave secreta. Esta clave se utiliza para cifrar y descifrar el mensaje. DES también puede utilizarse par el cifrado efectuado por un solo usuario como, por ejemplo, para almacenar archivos cifrados en un disco duro. DES tiene un tamaño de bloque de 64 bits y utiliza una clave de 56 bits durante el cifrado. Originalmente se diseñó para su implementación en el hardware. Cada cinco años, NIST confirma de nuevo a DES como estándar de cifrado oficial del gobierno del los Estados Unidos.

DER. Distinguished Encoding Rules.

DES. Data Encryption Standard.

descifrar. Deshacer el proceso de cifrado.

Directorio. Estructura jerárquica que se utiliza como depósito global de información relacionada con comunicaciones (como, por ejemplo, correo electrónico o intercambios cifrados). El Directorio almacena elementos específicos esenciales para la estructura PKI, incluidos claves públicas, certificados y listas de revocación de certificados.

Los datos del Directorio están organizados jerárquicamente en forma de árbol, con la raíz en la parte superior del árbol. Frecuentemente, las organizaciones de los niveles más altos representan países, gobiernos o empresas. Los usuarios y

dispositivos suelen representarse como hojas de cada árbol. Cada usuario, organización, localidad, país o dispositivo tiene su propia entrada. Cada entrada está formada por atributos escritos que proporcionan información sobre el objeto que representa la entrada.

Cada entrada del Directorio está unida a un nombre distinguido (DN) asociado a ella. Dicho nombre es exclusivo cuando la entrada incluye un atributo que es exclusivo para el objeto en el mundo real. Vea el siguiente ejemplo de DN: en él, el país (C) es EE UU, la organización (O) es IBM, la unidad de organización (OU) es Trust y el nombre común (CN) es CA1.

```
C=US/O=vnet/OU=Trust/CN=CA1
```

Distinguished Encoding Rules (DER). DER selecciona únicamente un tipo de codificación entre los permitidos por las normas de codificación, eliminando de este modo todas las opciones del remitente.

DN. Nombre distinguido.

dominio. *Vea* dominio seguro *y* dominio de registro.

dominio de registro. Conjunto de políticas, recursos y opciones de configuración relacionados con procesos de registro de certificados específicos. El nombre del dominio es un subconjunto de los URL utilizados para ejecutar la aplicación de registro.

dominio fiable. Conjunto de entidades cuyos certificados han sido certificados por la misma CA.

dominio seguro. Grupo (empresa, grupo o equipo de trabajo, docente o gubernamental) cuyos certificados han sido emitidos por la misma CA. Los usuarios que tengan certificados firmados por una CA puede considerar fiable la identidad de otro usuario que tenga un certificado firmado por la misma CA.

E

e-business. Transacciones comerciales a través de redes y de sistemas. Incluye la compra y venta de mercancías y servicios. También incluye la transferencia de fondos a través de comunicaciones digitales.

e-commerce. Transacciones de empresa a empresa. Incluye la compra y venta de mercancías y servicios (con cliente, distribuidores, proveedores y demás) en Internet. Es un elemento primario de e-business.

entidad final. El sujeto de un certificado que no es un CA.

esquema. Cuando está relacionado con IBM SecureWay Directory, estructura interna que define las relaciones entre distintos tipos de objetos.

estructura interna. *Vea* esquema.

extensión de certificado. Característica opcional del formato del certificado X.509v3 que permite la inclusión de campos adicionales en el certificado. Hay extensiones estándar y extensiones definidas por el usuario. Hay extensiones estándar para varias finalidades como, por ejemplo, información sobre claves y políticas, atributos de sujeto y emisor y limitaciones en la vía de certificación.

extranet. Un derivado de Internet que utiliza una tecnología similar. Las empresas están empezando a utilizar la divulgación, el comercio electrónico, la transmisión de mensajes y el groupware en la Web para varias comunidades de clientes, asociados y personal interno.

F

File Transfer Protocol (FTP). Protocolo de cliente/servidor de Internet que se utiliza para transferir archivos entre sistemas.

firma digital. Mensaje codificado añadido a un documento o a datos que garantiza la identidad del remitente.

Una firma digital puede proporcionar un nivel de seguridad superior al de un firma física. Esto se debe a que una firma digital no es un nombre cifrado ni una serie de simples códigos de identificación. De hecho, es un resumen cifrado del mensaje que se está firmando. Por lo tanto, al unir una firma digital a un mensaje se proporciona una sólida identificación del remitente. (Únicamente la clave del remitente puede crear la firma.) También fija el contenido del mensaje que va a firmarse (el resumen del mensaje cifrado debe coincidir con el contenido del mensaje o la firma no será válida). Por lo tanto, la firma digital no puede copiarse de un mensaje y aplicarse a otro ya que, entonces, el resumen (o ″hash″) no coincidiría. Cualquier alteración del mensaje firmado invalidará la firma.

firmar. Utilizar la clave privada para generar una firma. La firma es un medio de probar que se es el responsable y se aprueba el mensaje que se está firmando.

firma y verificación. Firmar es utilizar un clave privada digital para generar una firma. Verificar es utilizar la clave pública correspondiente para verificar la firma.

FTP. File Transfer Protocol.

H

historia de acciones. Los sucesos acumulados en el ciclo de vida de una credencial.

HTML. Hypertext Markup Language.

HTTP. Hypertext Transaction Protocol.

Hypertext Markup Language (HTML). Lenguaje de marcación para la codificación de páginas Web. Se basa en SGML.

hypertexto. Texto que contiene palabras, frases o gráficos en los que el lector puede pulsar el botón del ratón para recuperar y visualizar otro documento. Esas palabras, frases o gráficos se denominan hiperenlaces. Su recuperación se denomina enlace.

Hypertext Transaction Protocol (HTTP). Protocolo de cliente/servidor de Internet para transferir archivos en hypertexto a través de la Web.

I

ICL. Lista de certificados emitidos

ID de petición. Valor ASCII de 24 a 32 caracteres que identifica de forma exclusiva una petición de certificado a la RA. Este valor puede utilizarse en la transacción de petición de certificado para recuperar el estado de la petición o el certificado asociado a la misma.

instancia. En DB2, una instancia es un entorno de gestión de base de datos para almacenar datos y ejecutar aplicaciones. Permite la definición de un conjunto común de parámetros de configuración para varias bases de datos.

integridad. Un sistema protege la integridad de los datos si impide su modificación on autorizada (lo contrario sería proteger la confidencialidad de los datos impidiendo su divulgación no autorizada).

interfaz de programas de aplicación (API). En Policy Director, interfaz funcional que permite a un programa de aplicación escrito en lenguaje de alto nivel utilizar funciones específicas de Policy Director. La API de autorizaciones de Policy Director basada en estándares permite a las aplicaciones efectuar llamadas al Policy Director Authorization Service centralizado. Al realizar estas llamadas se elimina la necesidad de que los programadores deban escribir un código de autorización para cada nueva aplicación. La API de autorizaciones de Policy Director permite a las empresas estandarizar todas las aplicaciones sobre una infraestructura de autorizaciones fiable. Con la API de autorizaciones de Policy Director, las empresas pueden proporcionar más control para el acceso a recursos de sus redes. En el manual *Policy Director Programmer's Guide and Reference* puede ver las descripciones de la API de autorizaciones de Policy Director.

Internet. Grupo de redes a nivel mundial que proporciona una conexión electrónica entre sistemas. Permite a los sistemas comunicarse mediante dispositivos de software como el correo electrónico o los navegadores Web. Por ejemplo, algunas universidades están en una red que, a su vez, se enlaza con otras redes similares para formar Internet.

Intervalo de publicación de CRL. Definido en el archivo de configuración de la CA, es el intervalo de tiempo entre publicaciones periódicas de la CRL en el Directorio.

intranet. Red dentro de una empresa que reside normalmente detrás de los cortafuegos. Es un derivado de Internet y utiliza una tecnología similar. Técnicamente, la intranet es una mera ampliación de Internet. HTML y HTTP son algunos de los elementos comunes.

IPSec. Norma de seguridad de protocolos de Internet (Internet Protocol Security) desarrollada por IETF. IPSec es un protocolo de la capa de la red, diseñado para proporcionar servicios seguridad mediante cifrado que admite de forma flexible combinaciones de autentificación, integridad, control de accesos y confidencialidad. Debido a sus fuertes características de autentificación, ha sido adoptada por muchos proveedores de productos de VPN como protocolo para establecer conexiones punto a punto seguras a través de Internet.

J

Java. Conjunto de tecnologías informáticas preparadas para la red y no dirigidas a plataformas específicas desarrolladas por Sun Microsystems, Incorporated. El entorno de Java está formado por el sistema operativo de Java, las máquinas virtuales para distintas plataformas, el lenguaje de programación orientado a objetos de Java y varias clases de bibliotecas.

Java Virtual Machine (JVM). Parte del entorno de ejecución de Java responsable de interceptar códigos de byte.

L

LDAP. Lightweight Directory Access Protocol.

lenguaje Java. Lenguaje de programación desarrollado por Sun Microsystems y diseñado específicamente para ser utilizado en aplicaciones applets y agente.

Lightweight Directory Access Protocol (LDAP). Protocolo utilizado para acceder al Directorio.

lista de certificados emitidos (ICL). La lista completa de los certificados que han sido emitidos y su estado actual. Los certificados están ordenados por número de serie y estado. Es la CA quien mantiene esta lista que se almacena en la base de datos de la CA.

lista de control de accesos (ACL). Mecanismo para limitar la utilización de un recurso específico a usuarios autorizados.

lista de revocación de certificados (CRL). Una lista de certificados firmados digitalmente y con indicación de

la hora que la autoridad de certificación ha revocado. Los certificados de la lista debe considerarse inaceptables. *Vea también* certificado digital

M

MIME (Multipurpose Internet Mail Extensions). Conjunto de especificaciones disponible sin cargos que permite el intercambio de texto en distintos lenguajes con juegos de caracteres diferentes. También permite el correo multimedia entre muchos sistemas informáticos distintos que utilicen los estándares de correo de Internet. Por ejemplo, los mensajes de correo electrónico pueden contener juegos de caracteres distintos de los de US-ASCII, texto enriquecido, imágenes y sonido.

modelo de fiabilidad. Convenio de estructuración que indica la forma en que unas autoridades de certificación certifican a otras autoridades.

N

National Security Agency (NSA). Entidad oficial de seguridad del gobierno de los Estados Unidos.

navegador. *Vea*navegador Web.

navegador Web. Software cliente que se ejecuta en un PC de sobremesa y permite al usuario examinar páginas de la World Wide Web o HTML locales. Es una herramienta de recuperación que proporciona acceso universal a la gran cantidad de material hypermedia disponible en la Web y en Internet. Algunos navegadores pueden visualizar texto y gráficos y otros sólo pueden visualizar texto. La mayoría de navegadores pueden manejar las formas más importantes de comunicación de Internet, como, por ejemplo, transacciones FTP.

NLS. Soporte de idiomas nacionales.

nombre distinguido (DN). El nombre exclusivo de una entrada de datos almacenada en el Directorio. El DN identifica de forma exclusiva la posición de una entrada en la estructura jerárquica del Directorio.

no repudio. Utilización de una clave privada digital para impedir que el firmante de un documento niegue falsamente haberlo firmado.

O

objeto. En el diseño o programación orientado a objetos, una abstracción que encapsula datos y las operaciones relacionadas con dichos datos. *Vea también* clase.

P

par de claves. Claves correspondientes que se utilizan en el cifrado asimétrico. Una clave se utiliza para cifrar y la otra para descifrar.

par de claves pública/privada. Un par de claves pública/privada es una parte del concepto de cifrado con par de claves (presentado en 1976 por Diffie y Hellman para resolver el problema de la gestión de claves). En este planteamiento, cada persona obtiene un par de claves, la clave pública y la clave privada. La clave pública de cada persona se hace pública, mientras que la clave privada se mantiene secreta. No es necesario que el remitente y el receptor compartan la información secreta: todas las comunicaciones implican únicamente claves públicas y las claves privadas no se comparten ni se transmiten nunca. Ya no es necesario considerar fiable un canal de comunicaciones para asegurarse contra escuchas o revelaciones indiscretas. El único requisito que es necesario observar es que las claves públicas deben estar asociadas a sus usuarios de forma fiable (autentificadas, por ejemplo, en un directorio fiable). Cualquiera puede enviar mensajes confidenciales utilizando información pública. Sin embargo, el mensaje sólo podrá ser descifrado con la clave privada, que únicamente posee el destinatario. Además, el cifrado con par de claves no sólo puede utilizarse por su privacidad (cifrado), sino por su autentificación (firmas digitales).

pasarela. Unidad funcional que permite que redes o aplicaciones incompatibles se comuniquen.

PEM. Privacy-Enhanced Mail.

perfil de certificado. Conjunto de características que define el tipo de certificado que se desea (como, por ejemplo, certificados SSL o certificados IPSec). El perfil ayuda a gestionar la especificación y registro de certificados). El emisor puede cambiar los nombres de los perfiles y especificar las características del certificado que desea como, por ejemplo, el periodo de validez, la utilización de claves, las limitaciones de nombre distinguido (DN), etc.

PKCS. Public Key Cryptography Standards.

PKCS#10. *Vea* Public Key Cryptography Standards.

PKCS#12. *Vea* Public Key Cryptography Standards.

PKI. Public Key Infrastructure.

PKIX. Una PKI basada en X.509v3.

política de certificado. Conjunto de normas con nombre que indica la posibilidad de aplicación de un certificado a una determinada clase de aplicaciones que tengan requisitos comunes de seguridad. Por ejemplo, una política de certificado podría indicar si un tipo de

certificación determinado permite a un usuario realizar transacciones de mercancías dentro de un determinado rango de precio.

privacidad. Protección contra la divulgación no autorizada de datos.

Privacy-Enhanced Mail (PEM). El estándar de Internet para mejorar la privacidad del correo, que adoptó el Internet Architect Board (IAB) para proporcionar un correo electrónico seguro a través de Internet. Los protocolos PEM proporcionan cifrado, autentificación, integridad de mensajes y gestión de claves.

protocolo. un convenio aceptado para la comunicación entre sistemas.

protocolo de gestión de certificados (Certificate Management Protocol, CMP) PKIX. Protocolo que permite conexiones con aplicaciones que cumplan con las normas PKIX. PKIX CMP utiliza TCP/IP como mecanismo de transporte primario, aunque existe una capa de abstracción sobre los sockets. Esto permite el soporte de transportes de sondeo adicionales.

Public Key Cryptography Standards (PKCS). Normas informales entre proveedores desarrolladas en 1991 por RSA Laboratories con representantes de distintos proveedores informáticos. Estas normas incluyen el cifrado RSA, el acuerdo Diffie-Hellman, el cifrado basado en contraseñas, la sintaxis ampliada de certificados, la sintaxis de información de claves privadas y la sintaxis de certificaciones.

- PKCS#10 especifica una sintaxis estándar para peticiones de certificación.
- PKCS#12 especifica un formato portátil para almacenar o transportar claves privadas, certificados, diversos elementos secretos, etc.

Public Key Infrastructure (PKI). Norma para el software de seguridad basado en el cifrado de claves pública. PKI es un sistema de certificados digitales, autoridades de certificación, autoridades de registro, servicios de gestión de certificados y servicios de directorios distribuidos. Se utiliza para verificar la identidad y la autoridad de las partes implicadas en cualquier transacción a través de Internet. Estas transacciones pueden implicar operaciones en las que se requiera una verificación de la identidad. Por ejemplo, pueden confirmar el origen de ofertas, autores de mensajes de correo electrónico o transacciones financieras.

PKI lleva esta operación a cabo permitiendo la utilización de claves públicas de cifrado y de certificados de usuarios para que un individuo u organización pueda efectuar la autentificación. Proporciona directorios en línea que contienen claves públicas de cifrado y certificados que se utilizan para verificar certificados digitales, credenciales y firmas digitales.

PKI es un medio para lograr respuestas rápidas y eficaces para la verificación de consultas y respuestas sobre claves públicas de cifrado. También identifica posibles riesgos en la seguridad del sistema y mantiene recursos para resolver infracciones en la seguridad. Por último, PKI proporciona un servicio de indicación digital de la hora para transacciones comerciales importantes.

R

RA. Autoridad de registro.

RC2. Cifrado de bloque de tamaño variable de clave, diseñado por Ron Rivest para RSA Data Security. *RC* siglas de *Ron's Code* o *Rivest's Cipher*. Es más rápido que DES y se ha diseñado como posible sustituto de DES. Puede hacerse más o menos seguro debido a que efectúa una búsqueda de claves, más exhaustiva que la de DES, utilizando los tamaños de claves adecuados. Tiene un tamaño de bloque de 64 bits y su software es dos o tres veces más rápido que DES. RC2 puede utilizarse en las mismas modalidades que DES.

Un acuerdo entre Software Publishers Association (SPA) y el gobierno de los Estados Unidos proporciona a RC2 un estado especial. Esto hace que el proceso de aprobación de la exportación sea más simple y rápido que el proceso de exportación cifrado habitual. Sin embargo, para que sea posible la aprobación de exportación rápida de un producto, el tamaño de la clave RC2 debe ser inferior a 40 bits, con algunas excepciones. Puede utilizarse una cadena de caracteres adicional para frustrar contra posibles cifrados los intentos de calcular previamente una tabla de búsqueda grande.

RC4. Cifrado de bloque de tamaño variable de clave, diseñado por Ron Rivest para RSA Data Security. *RC* siglas de *Ron's Code* o *Rivest's Cipher*. Es parecido a RC2, pero su tamaño de bloque es de 128 bits.

registro previo. En IBM SecureWay Trust Authority, proceso que permite a un usuario, normalmente un administrador, inscribir a otros usuarios. Si el solicitante se aprueba, la autoridad de registro (Registration Authority, RA) proporciona información que permite al usuario obtener posteriormente el certificado utilizando la aplicación de cliente de la autoridad fiable (Trust Authority).

repudiar. Rechazar como falso; por ejemplo, negar que se ha enviado un mensaje específico o se ha sometido una petición específica.

S

Secure Sockets Layer (SSL). Protocolo de comunicaciones IETF estándar que tiene incorporados servicios de seguridad tan transparentes como es

posible para el usuario final. Proporciona un canal digital de comunicaciones seguro.

Normalmente, un servidor habilitado para SSL acepta peticiones peticiones de conexión SSL en distintas puertas que las peticiones de HTTP estándar. SSL crea una sesión durante la cual las señales de intercambio para establecer las comunicaciones entre dos módems se producen una sola vez. Después de esto, la comunicación se cifra. La comprobación de la integridad de los mensajes continúa hasta que finaliza la sesión SSL.

seguimiento de auditoría. Datos en forma de vía de acceso lógica que enlaza una secuencia de sucesos. Un seguimiento de auditoría permite realizar el rastreo de las transacciones o de la historia de una determinada actividad.

servidor. (1) En una red, estación de datos que proporciona funciones a otras estaciones. Por ejemplo, un servidor de archivos. (2) En TCP/IP, sistema de una red que gestiona las peticiones de un sistema a otra ubicación, llamada cliente/servidor.

servidor CAS. El servidor para el componente Credentials Acquisition Service (CAS) de Policy Director.

servidor de auditoría. Servidor que recibe sucesos de auditoría de clientes de auditoría y los graba en una anotación cronológica de auditoría.

servidor HTTP. Servidor que gestiona comunicaciones basadas en la Web con navegadores y demás programas de una red.

servidor proxy. Intermediario entre el sistema que solicita acceso (sistema A) y el sistema al que se accede (sistema B). Por lo tanto, si un usuario efectúa una petición de un recurso para el sistema A, la petición se dirige a un servidor proxy. El servidor proxy efectúa la petición, obtiene la respuesta del sistema B y, a continuación, envía la respuesta al usuario final. Los servidores proxy resultan útiles para acceder a recursos de la World Wide Web desde dentro de un cortafuego.

servidor Web. Programa servidor que responde a peticiones de recursos de información procedentes de programas de navegador. *Vea también* servidor.

servlet. Programa del área del servidor que proporciona más funcionalidad a los servidores habilitados para Java.

SGML. Standard Generalized Markup Language.

signatura de código. Técnica para firmar programas ejecutables con firmas digitales. La finalidad de la signatura de código es mejorar la fiabilidad del software que se distribuye por Internet.

Simple Mail Transfer Protocol (SMTP). Protocolo que transfiere correo electrónico a través de Internet.

S/MIME. Estándar que tiene soporte para la firma y cifrado del correo electrónico transmitido a través de Internet. *Vea* MIME.

SMTP. Simple Mail Transfer Protocol.

Soporte de Idiomas Nacionales (National Language Support, NLS). Soporte que se encuentra dentro de un producto para controlar las diferencias de soportes nacionales (locales) como, por ejemplo, el idioma, la moneda, el formato de fecha y hora y la presentación numérica.

SSL. Secure Sockets Layer.

Standard Generalized Markup Language (SGML). Estándar para la descripción de lenguajes de marcación. HTML está basado en SGML.

T

TCP/IP. Transmission Control Protocol/Internet Protocol.

texto normal. Datos que no están cifrados. *Sinónimo de* texto plano.

texto plano. Datos que no están cifrados.*Sinónimo de* texto normal.

tipo. *Vea* tipo de objeto.

tipo de objeto. La clase de objeto que puede almacenarse en IBM SecureWay Directory. Por ejemplo, una empresa, sala de reuniones, dispositivo, persona, programa o proceso.

Transmission Control Protocol/Internet Protocol (TCP/IP). Conjunto de protocolos de comunicación que tiene soporte para funciones de conectividad de igual a igual para redes de área local y de área amplia.

triple DES. Algoritmo simétrico que cifra tres veces el texto planto. Aunque esta operación puede hacerse de muchas maneras, la forma más segura de cifrado múltiple es la de DES con tres claves distintas.

Trust Authority. Solución integrada de IBM SecureWay que tiene soporte para la emisión, renovación y revocación de certificados digitales. Estos certificados pueden utilizarse en una amplia gama de aplicaciones de Internet y proporcionan un medio de autentificar usuarios y de asegurar comunicaciones fiables.

túnel. En tecnología VPN, conexión virtual punto a punto que se realiza ″a petición″ a través de Internet. Cuando están conectados, los usuarios pueden utilizar el túnel para intercambiar información segura, cifrada y encapsulada con servidores de la red empresarial privada.

U

Unicode. Conjunto de caracteres de 16 bits definido mediante ISO 10646. El estándar de codificación de caracteres de Unicode es un código de caracteres internacional para el proceso de información. El estándar Unicode abarca los principales scripts del mundo y es el fundamento para la internacionalización y localización del mundo. Todo el código fuente de un entorno de programación Java está escrito en Unicode.

Uniform Resource Indicator (URI). Un URL absoluto indica una posición de URI en relación con un nombre de SISTEMA PRINCIPAL o una dirección IP y una puerta de red.

Uniform Resource Locator (URL). Esquema para el direccionamiento de recursos en Internet. El URL especifica el protocolo y el nombre del sistema principal o la dirección IP. Incluye también el número de puerta, la vía de acceso y detalles sobre el recurso necesarios para acceder a un recurso desde una máquina determinada.

URI. Uniform Resource Indicator.

URL. Uniform Resource Locator.

UTF-8. Formato de transformación. Permite el que los sistemas de proceso de la información que sólo manejan juegos de caracteres de 8 bits conviertan el Unicode de 16 bits en un equivalente de 8 bits y viceversa, sin que se pierda información.

V

validación encadenada. Validación de todas las firmas de CA de la jerarquía de fiabilidad a través de la cual se emitió un certificado determinado. Por ejemplo, si a una CA le emitió su certificado de signatura otra CA, ambas signaturas se validarán durante la validación del certificado presentado por el usuario.

Virtual Private Network (VPN). Red privada de datos que, para establecer conexiones remotas, utiliza Internet en vez de líneas telefónicas. Como los usuarios acceden a recursos de la red empresarial a través de un proveedor de servicios de Internet (Internet Service Provider, ISP) en vez a través de una compañía telefónica, las empresas pueden reducir significativamente los costes de los accesos remotos. Una VPN también mejora la seguridad de los intercambios de datos. En la tecnología de cortafuego tradicional, el contenido del mensaje puede cifrarse, pero no así las direcciones de origen y destino. Con la tecnología VPN, los usuarios pueden establecer una conexión de túnel en la que se cifra y encapsula todo el paquete de información (contenido y cabecera).

VPN. Virtual Private Network.

W

World Wide Web (WWW). Parte de Internet en la que se establece una red de conexiones entre sistemas que contienen materiales hypermedia. Estos materiales proporcionan información y pueden proporcionar enlaces con otros materiales de la WWW e Internet. Se accede a los recursos de la WWW mediante un programa navegador Web.