IBM& SecureWay Policy Director

Installation und Konfiguration

Version 3 Release 0

IBM& SecureWay Policy Director

Installation und Konfiguration

Version 3 Release 0

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen in Anhang A, „Bemerkungen“ auf Seite 93 gelesen werden.

Diese Ausgabe bezieht sich auf Version 3, Release 0.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM SecureWay Policy Director Up and Running,
IBM Part Number CT63KNA,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW NLS Center
Kst. 2877
Oktober 1999

Inhaltsverzeichnis

Zu diesem Handbuch

Dieses Handbuch stellt Informationen über die Installation und Konfiguration von IBM& SecureWay& Policy Director (Policy Director) zur Verfügung. Die Policy Director-Server können unter den folgenden Betriebssystemen installiert werden:

- Microsoft& Windows NT&
- AIX&
- Solaris&

Der NetSEAT-Client kann unter den folgenden Betriebssystemen installiert werden:

- Windows& 95
- Windows 98
- Windows NT

Zielgruppe

Dieses Handbuch ist für den Administrator bestimmt, der für die Planung und Installation von Policy Director zuständig ist.

Der Administrator sollte Kenntnisse in der Installation und Konfiguration von IBM Distributed Computing Environment (DCE) und IBM SecureWay Directory LDAP (Lightweight Directory Access Protocol) haben. Die IBM SecureWay Directory und IBM Distributed Computing Environment Server werden von Policy Director verwendet und sind Bestandteil des Policy Director-Produkts.

Aufbau dieses Handbuchs

Dieses Handbuch enthält folgende Kapitel:

- „Erläuterungen zu Policy Director“ auf Seite 1, gibt eine Übersicht über Policy Director und die zugehörigen Komponenten.
- „Systemvoraussetzungen“ auf Seite 15, enthält Informationen über die Software- und Hardwarevoraussetzungen, die Ihre Betriebsumgebung erfüllen muß.
- „Planung für Policy Director“ auf Seite 19, stellt Informationen über die Planung, Organisation und Verwaltung von Policy Director zur Verfügung.
- „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29, enthält Informationen über die Installation und Konfiguration von IBM SecureWay Directory Version 3.1.1 (LDAP) Client SDK und Server, wenn Sie die LDAP-Benutzerregistrierungsdatenbank auswählen. Sie müssen den LDAP-Server installieren und konfigurieren, bevor Sie Policy Director installieren. Außerdem muß der LDAP-Server aktiv sein, bevor Policy Director installiert wird.

- „Installation von Policy Director für Windows“ auf Seite 45, beschreibt die Installation und Konfiguration von Policy Director unter dem Betriebssystem Windows NT.
- „Installation von Policy Director für AIX“ auf Seite 59, beschreibt die Installation und Konfiguration von Policy Director unter dem IBM Betriebssystem AIX.
- „Installation von Policy Director für Solaris“ auf Seite 75, beschreibt die Installation und Konfiguration von Policy Director unter dem Betriebssystem Sun Solaris.
- „Referenzliteratur“ auf Seite 89, enthält Informationen über andere Dokumentationen zu Policy Director und über Dokumentationen zu zugehörigen Produkten.

Neue Funktionen in diesem Release

In diesem Release von Policy Director sind die folgenden neuen Funktionen enthalten:

- Unterstützung für IBM SecureWay Directory bei der Speicherung von Informationen über Benutzer- und Gruppenberechtigungen.
- Die letzten Aktualisierungen der Berechtigungs-API-Spezifikation aus der Open Group.
- Möglichkeit zum Definieren und Bearbeiten von Proxy-Benutzerberechtigungen in IBM Firewall unter Verwendung der Policy Director-Verwaltungskonsole.
- Policy Director Credentials Acquisition Service (CAS), der Unterstützung für die Verwendung von externen Authentifizierungsservices zur Verfügung stellt.
- Unterstützung für zertifikatsgestützte Authentifizierung auf der Client-Seite unter Verwendung des neuen Policy Director Credentials Acquisition Service.
- Möglichkeit zum Schreiben eines eigenen angepaßten CAS (Credentials Acquisition Service) unter Verwendung der IDL-Schnittstelle (Interface Definition Language - Schnittstellendefinitionssprache) zwischen WebSEAL und Policy Director CAS. Policy Director stellt auch das allgemeine Server-Gerüst zur Verfügung, das die Ausführung von Policy Director CAS-Server-Funktionen, wie beispielsweise Systemstart, Server-Registrierung und Signalverarbeitung, ermöglicht.
- Möglichkeit zur Verwendung eines SSL-Tunnelmechanismus (SSL = Secure Sockets Layer) neben der Verwendung des GSS-Tunnelmechanismus (GSS = Generic Security Services).
- Verwendung der Policy Director-Befehlszeilenschnittstelle zur Verwaltung von Anmelde- und Kennwortmaßnahmen.
- Verwendung der Policy Director-Verwaltungskonsole oder der Befehlszeilenschnittstelle zur Verwaltung von Benutzern, Gruppen und Ressourcen (Zielen) mit Einzelanmeldung.
- Web-gestütztes Kennwortverwaltungs-Tool für Ressourcen mit Einzelanmeldung.
- Integrierter Installationsprozeß.

Jahr 2000

Die IBM Produkte sind Jahr-2000-fähig, d. h., sie sind bei Benutzung gemäß der dazugehörigen IBM Dokumentation in der Lage, Datumsdaten innerhalb des 20. und 21. Jahrhunderts und zwischen diesen beiden Jahrhunderten korrekt zu verarbeiten, bereitzustellen oder zu empfangen, vorausgesetzt, daß alle anderen Produkte (z. B. Hardware, Software, Firmware), die zusammen mit ihnen benutzt werden, richtige Datumsdaten ordnungsgemäß mit ihnen austauschen.

Service und Unterstützung

Benachrichtigen Sie IBM bezüglich Service und Unterstützung für alle Produkte, die in IBM SecureWay FirstSecure enthalten sind. Einige dieser Produkte verweisen möglicherweise auf Nicht-IBM-Unterstützung. Erhalten Sie diese Produkte als Teil des FirstSecure-Programmpakets, benachrichtigen Sie IBM bezüglich Service und Unterstützung.

Konventionen

In diesem Handbuch werden die folgenden typografischen Konventionen verwendet:

Konvention	Bedeutung
Fett	Benutzerschnittstellenelemente, wie beispielsweise Kontrollkästchen, Schaltflächen und Einträge in Listenfenstern.
`Monospace-Schrift`	Syntax, Beispielcode und jeder Text, der vom Benutzer eingegeben werden muß.
Kursiv	Hervorhebung und erste Verwendung von speziellen Begriffen, die in Policy Director von Bedeutung sind.
→	Zeigt eine Reihe von Auswahlmöglichkeiten in einem Menü. Auf **Datei** → **Ausführen** klicken bedeutet beispielsweise, daß Sie zuerst auf **Datei** und dann auf **Ausführen** klicken müssen.

Web-Informationen

Informationen über die neuesten Aktualisierungen in Policy Director können über die folgende Web-Adresse angefordert werden:

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

Informationen über Aktualisierungen in anderen Produkten von IBM SecureWay FirstSecure können über die folgende Web-Adresse angefordert werden:

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

Erläuterungen zu Policy Director

IBM SecureWay Policy Director (Policy Director) ist entweder als Komponente von IBM SecureWay FirstSecure oder als eigenständiges Produkt verfügbar.

Was ist IBM SecureWay FirstSecure?

IBM SecureWay FirstSecure (FirstSecure) ist Bestandteil der integrierten IBM Sicherheitslösungen. FirstSecure ist eine umfassende Gruppe integrierter Produkte, die Ihr Unternehmen wie folgt unterstützen:

- Erstellung einer sicheren e-business-Umgebung.
- Reduzierung des Gesamtaufwands für Eigentumsrechte bei der Sicherheit durch Vereinfachung der Sicherheitsplanung.
- Implementierung von Sicherheitsmaßnahmen.
- Erstellung einer effektiven e-business-Umgebung.

Zu den Produkten von IBM SecureWay gehören:

Policy Director
IBM SecureWay Policy Director (Policy Director) stellt Funktionen für die Authentifizierung, Berechtigung, Datensicherheit und Web-Ressourcenverwaltung zur Verfügung.

Boundary Server
IBM SecureWay Boundary Server (Boundary Server) stellt die folgenden Funktionen zur Verfügung:

- Die kritischen Firewall-Funktionen für Filtern, Proxy und Gateway auf Netzebene
- Eine VPN-Verbindung (VPN = Virtual Private Network) zu IBM Firewall
- Komponenten für die Internet-Sicherheit
- Eine Sicherheitslösung mit mobilem Code

Eine Konfigurations-GUI verbindet die Proxy-Benutzerfunktion von Policy Director mit dem Firewall-Produkt von Boundary Server.

Intrusion Immunity
Intrusion Immunity stellt eine Funktion zum Erkennen von Eindringlingen und einen Antivirus-Schutz zur Verfügung.

Trust Authority
IBM SecureWay Trust Authority (Trust Authority) unterstützt PKI-Standards (PKI = Public Key Infrastructure) für Kryptographie und Interoperabilität. Trust Authority bietet Unterstützung für die Ausgabe, die Erneuerung und den Widerruf von digitalen Zertifikaten. Diese Zertifikate bieten die Möglichkeit, Benutzer zu authentifizieren und eine gesicherte Kommunikation sicherzustellen.

Toolbox IBM SecureWay Toolbox (Toolbox) ist eine Gruppe von Anwendungsprogrammierschnittstellen (APIs), mit denen Anwendungsprogrammierer Sicherheit in ihre Software integrieren können. Sie können die Toolbox als Teil von FirstSecure anfordern. Sowohl Policy Director als auch die Toolbox enthalten die Policy Director API-Bibliothek und -Dokumentation.

Da jedes Produkt von IBM SecureWay FirstSecure unabhängig voneinander installiert werden kann, können Sie eine gesteuerte Umstellung auf eine gesicherte Umgebung planen. Mit dieser Fähigkeit lassen sich Komplexität und Kosten für das Sichern Ihrer Umgebung reduzieren und der Einsatz von Web-Anwendungen und -Ressourcen beschleunigen.

Die FirstSecure-Dokumentation *Planung und Integration* enthält weitere Informationen über die Komponenten von FirstSecure sowie eine Auflistung der Produktdokumentation zu IBM SecureWay.

Was ist IBM SecureWay Policy Director?

Policy Director ist eine eigenständige Berechtigungs- und Sicherheitsverwaltungslösung, die Endpunkt-zu-Endpunkt-Sicherheit für Ressourcen über geografisch verteilte Intranets und *Extranets* zur Verfügung stellt. Ein *Extranet* ist ein Virtual Private Network (VPN), das Zugriffssteuerungs- und Sicherheitseinrichtungen verwendet, um die Verwendung eines oder mehrerer Intranets, die an das Internet angeschlossen sind, auf ausgewählte Subskribenten zu beschränken.

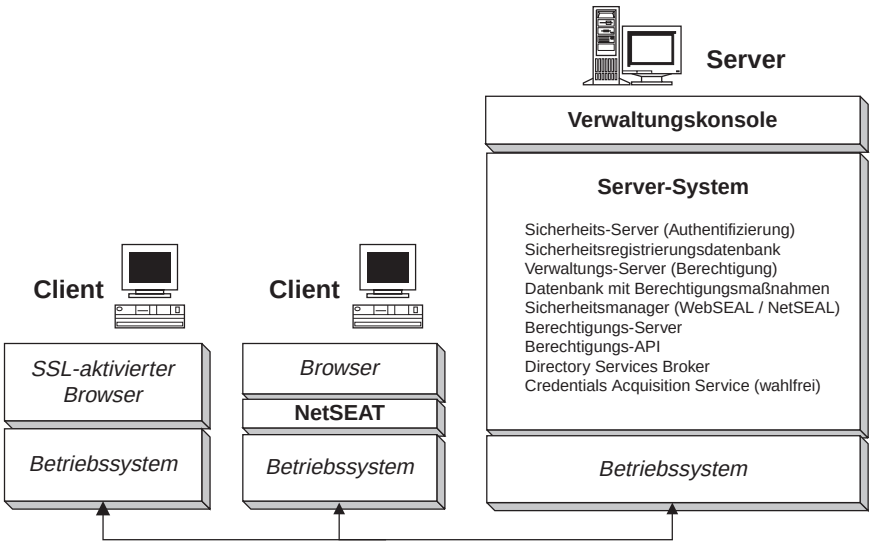
Policy Director stellt Services für die Authentifizierung, Berechtigung, Datensicherheit und Ressourcenverwaltung zur Verfügung. Sie können Policy Director zusammen mit Internet-gestützten Standardanwendungen verwenden, um sichere und gut verwaltete Intranets und Extranets aufzubauen.

Policy Director kann unter den Betriebssystemen Windows NT, AIX und Solaris ausgeführt werden.

Komponenten von Policy Director

Policy Director enthält die folgenden Komponenten:

- IBM SecureWay Directory LDAP (Lightweight Directory Access Protocol) und IBM Distributed Computing Environment (DCE) Clients und Server
- Policy Director-Basis
- Verwaltungs-Server
- Sicherheitsmanager, bestehend aus WebSEAL und NetSEAL
- Credential Acquisition Service (CAS)
- Berechtigungs-Server
- Berechtigungs-API (Anwendungsprogrammierschnittstelle)
- NetSEAT-Client
- Verwaltungskonsole
- Directory Services Broker (DSB)



Bevor Sie Policy Director installieren, müssen Sie bestimmen, welche Sicherheitsvoraussetzungen und Verwaltungsfähigkeiten für Ihr Netz erforderlich sind. Entscheiden Sie anhand der folgenden Abschnitte, welche Komponenten von Policy Director benötigt werden.

IBM SecureWay Directory und DCE Server

Die IBM SecureWay Directory und IBM Distributed Computing Environment Server werden von Policy Director verwendet und sind Bestandteil des Policy Director-Produkts.

Policy Director kann entweder eine LDAP-Benutzerregistrierungsdatenbank oder eine DCE-Benutzerregistrierungsdatenbank verwenden. Bei der Installation von Policy Director werden Sie aufgefordert, die Art der Benutzerregistrierungsdatenbank auszuwählen.

Soll eine LDAP-Benutzerregistrierungsdatenbank verwendet werden, müssen Sie einen LDAP-Client installieren und einen LDAP-Server konfigurieren, bevor Policy Director installiert wird. Befolgen Sie die Anweisungen in „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29. Soll eine DCE-Benutzerregistrierungsdatenbank verwendet werden, kann der Abschnitt über die Installation und Konfiguration von LDAP übersprungen werden.

IBM SecureWay Directory Server

SecureWay Directory stellt LDAP (Lightweight Directory Access Protocol) zur Verfügung, um Verzeichnisinformationen an einem zentralen Ort zum Speichern, Aktualisieren, Abrufen und Austauschen zu verwalten. Wird LDAP für die Benutzerregistrierungsdatenbank verwendet, verwendet Policy Director LDAP, um Benutzern eine Berechtigung zu erteilen.

IBM Distributed Computing Environment Server

Distributed Computing Environment (DCE) enthält Services und Tools, die die Erstellung, Verwendung und Verwaltung von verteilten Anwendungen in einer heterogenen Datenverarbeitungsumgebung unterstützen. DCE bildet die gesicherte Domäne, innerhalb der die Policy Director-Server gegenseitig den Benutzer authentifizieren und sicher miteinander kommunizieren können. Unter dem Betriebssystem Windows NT arbeitet der NetSEAT-Client als DCE-Client.

Policy Director-Basis

Die Policy Director-Basis (IVBase) ist die allgemeine Referenzsoftware, die von allen Policy Director-Komponenten verwendet wird. Diese Komponente wird automatisch installiert, wenn andere Policy Director-Komponenten installiert werden. Dies gilt jedoch nicht, wenn die Verwaltungskonsole unter Windows installiert wird.

Für AIX ist die SMIT-Setup-Komponente (IV.Smit) als Teil des IV.Base-Pakets eingeschlossen. Dieses Paket enthält Konfigurationsdaten, die von SMIT verwendet werden. Dieses Paket muß auf allen AIX-Servern installiert werden.

Verwaltungs-Server

Der Verwaltungs-Server (IVMgr) ist der primäre Berechtigungs-Server für die gesamte gesicherte Domäne. Der Verwaltungs-Server steuert und verwaltet die Hauptdatenbank mit Berechtigungsmaßnahmen. Alle Daten fließen durch den Verwaltungs-Server.

Der Verwaltungs-Server muß auf einem Computer in der gesicherten Domäne installiert sein, bevor die Sicherheitsmanager oder die Berechtigungs-Server installiert werden, aber nicht notwendigerweise auf demselben Computer. In einer bestimmten gesicherten Domäne darf nur ein Exemplar des Verwaltungs-Servers installiert sein.

Jedes Exemplar des Verwaltungs-Servers erfordert es, daß die folgenden Komponenten auf demselben Computer wie der Verwaltungs-Server installiert werden:

- DCE-Client
- LDAP-Client (wenn LDAP als Benutzerregistrierungsdatenbank verwendet wird)
- Policy Director-Basis
- Verwaltungs-Server

Sicherheitsmanager

Der Sicherheitsmanager (IVNet) wendet Zugriffssteuerungsmaßnahmen an, die auf Informationen aus einer Replikationsdatenbank mit Berechtigungsmaßnahmen basieren. Der Sicherheitsmanager enthält die folgenden Komponenten:

- WebSEAL für eine feinkörnige Zugriffssteuerung für HTTP (Hypertext Transfer Protocol) und HTTPS (Secure Sockets Layer-Schnittstelle)
- NetSEAL für eine grobkörnige Zugriffssteuerung für TCP/IP (Transmission Control Protocol/Internet Protocol)

Die Komponenten NetSEAL und WebSEAL sind für die Konfiguration und Aktivierung dieser standardmäßig inaktivierten Funktionen erforderlich.

WebSEAL

WebSEAL (IVWeb) ist die HTTP-Server-Komponente des Sicherheitsmanagers. WebSEAL ist ein gesicherter Web-Server, der HTTP-, HTTPS- und NetSEAT-Clients unterstützt. WebSEAL unterstützt zusammen mit dem Credential Acquisition Service (CAS) von Policy Director die X.509-zertifikatsgestützte Authentifizierung für einen Policy Director-Benutzer.

NetSEAL

NetSEAL (IVTrap) stellt eine grobkörnige Zugriffssteuerung für TCP/IP-Server zur Verfügung. NetSEAL steuert den Zugriff auf eine Gruppe konfigurierter Ports auf einem TCP/IP-Server.

Die Policy Director-Produktgruppe stellt Sicherheit für den Datenaustausch zwischen Client und Server im Internet und in privaten Intranets zur Verfügung. Policy Director NetSEAL und Policy Director WebSEAL sind Server-Produkte, die Netzdaten innerhalb von gesicherten Domänen, die von DCE definiert werden, steuern und verwalten.

Berechtigungs-Server

Der Berechtigungs-Server (IVAcld) bearbeitet Berechtigungsanforderungen von Anwendungen Dritter, die die Berechtigungs-API von Policy Director im Fernmodus verwenden. Der Berechtigungs-Server sollte auf mindestens einem Computer in der gesicherten Domäne für Anwendungen Dritter installiert sein.

Berechtigungs-API (Anwendungsprogrammierschnittstelle)

Die Policy Director-Komponente Authorization Application Development Kit oder ADK (IVAuthADK) enthält die Policy Director-Berechtigungs-API (Anwendungsprogrammierschnittstelle). Mit der API können Sie Anwendungen erstellen, die die Policy Director-Berechtigung verwenden.

Policy Director Application Development Kit (ADK) enthält einen Berechtigungs-API-Server (AuthAPI™), mit dem Entwickler Policy Director-Sicherheit und -Berechtigung direkt in Firmenanwendungen eingliedern können. Die Policy Director-Berechtigungs-API stellt einen Direktzugriff auf den Policy Director-Berechtigungsservice zur Verfügung. Die Verwendung dieser Berechtigungs-API bedeutet, daß Entwickler nicht mehr Berechtigungscode für jede Anwendung schreiben müssen.

ADK enthält C-Beispielprogramme.

Außerdem enthält ADK die Quelle für die Demonstrations-Server für den Policy Director Credential Acquisition Service (CAS) und den externen Berechtigungsservice.

NetSEAT-Client

Der Policy Director NetSEAT-Client ist ein Lightweight-Client für Windows 95, Windows 98 oder Windows NT. NetSEAT stellt gesicherte Übertragungskanäle für Policy Director-Server zur Verfügung.

Die NetSEAT-Client-Software ermöglicht Clients die Verknüpfung mit gesicherten Domänen und die Verwendung der erweiterten Sicherheitsservices, die von WebSEAL- und NetSEAL-Servern zur Verfügung gestellt werden. NetSEAT sichert die gesamte Netzkommunikation eines Clients und erlaubt eine Endpunkt-zu-Endpunkt-Verschlüsselung des gesamten Web-gestützten und Client/Server-Datenverkehrs.

NetSEAT bietet die Möglichkeit, den TCP/IP-Datenverkehr eines Clients, wie beispielsweise den durch Services wie Telnet und POP3 generierten Datenverkehr, zu sichern. NetSEAT ermöglicht einem Systemadministrator eine grobkörnige Steuerung der Netzaktivitäten einer Workstation. Diese Steuerung resultiert aus der Verwendung der Fähigkeit der gesicherten Domäne, Benutzer zu authentifizieren und Benutzern und Ressourcen Berechtigungen zuzuordnen.

Verwaltungskonsole

Die Verwaltungskonsole (IVConsole) ist eine Java-gestützte grafische Anwendung, mit der Sicherheitsmaßnahmen für die gesicherte Policy Director-Domäne verwaltet werden. Mit der Verwaltungskonsole können Sie Verwaltungs-Tasks für die Kontoregistrierungsdatenbank und die Hauptdatenbank mit Berechtigungsmaßnahmen ausführen. Die Verwaltungskonsole erfordert einen DCE-Client für die Anmeldung bei der gesicherten Domäne und für die Ausführung von gesicherten Fernprozeduraufrufen (Remote Procedure Calls = RPCs) an die Policy Director-Verwaltungs-Server. Die Verwaltungskonsole verwendet DCE-Lightweight-Services (Laufzeitservices), die von dem NetSEAT-Client unter Windows 95, Windows 98 oder Windows NT zur Verfügung gestellt werden.

Directory Services Broker

Der Directory Services Broker (DSB) wird als Teil der Verwaltungs-Server-Komponente verteilt. Die Verwaltungskonsole und NetSEAT-Clients benötigen einen DSB in der gesicherten Domäne, wenn sie auf einer Windows 95-, Windows 98- oder Windows NT-Workstation ausgeführt werden. Nach der Erstinstallation erfordert der DSB normalerweise keine Verwaltung oder Konfiguration.

Credentials Acquisition Service (wahlfrei)

Der Policy Director Credentials Acquisition Service (CAS) ist eine Komponente, die wahlweise konfiguriert werden kann.

Berechtigungsakquisition ist der Prozeß, bei dem bestimmte von einem Authentifizierungsmechanismus zur Verfügung gestellte Identitätsinformationen in eine allgemeine domänenweite Darstellung der Identität des Clients umgesetzt bzw. die Identitätsinformationen der Darstellung der Client-Identität zugeordnet werden. Diese allgemeine Darstellung wird als *Berechtigung des Clients* bezeichnet.

Wird die Berechtigungsakquisition oder -zuordnung benötigt, müssen Sie den Policy Director Credentials Acquisition Service zur Verwendung mit dem Policy Director WebSEAL-Server konfigurieren. Policy Director-Benutzer werden automatisch von WebSEAL Berechtigungen zugeordnet.

Für Clients, die mit Hilfe von X.509-Zertifikaten auf Client-Seite auf Policy Director zugreifen, können *Zertifikats*informationen Policy Director-Identitäten zugeordnet werden, indem der Policy Director Credentials Acquisition Service verwendet oder ein eigener Berechtigungsakquisitionsservice geschrieben wird.

Sind Benutzer in einer anderen externen Registrierungsdatenbank definiert, können die Benutzernamen mit Hilfe eines angepaßten CAS-Servers Policy Director-Identitäten zugeordnet werden. Sie können Ihren eigenen CAS-Server schreiben und anpassen, um eine spezifische Lösung für die gesicherte Domäne zur Verfügung zu stellen und Authentifizierungsinformationen, wie beispielsweise Client-Zertifikate, Benutzernamen oder Token, zu verarbeiten. Der Entwickler oder Designer des Policy Director Credentials Acquisition Service legt die gesamten Spezifikationen dieses Authentifizierungs- und Zuordnungsservices fest. Policy Director speichert Zuordnungsregeln in einer Datenbank außerhalb von Policy Director. Policy Director stellt die IDL-Schnittstelle (Interface Definition Language - Schnittstellendefinitionssprache) zwischen WebSEAL und dem Policy Director Credentials Acquisition Service zur Verfügung. Policy Director stellt außerdem das allgemeine Server-Gerüst zur Verfügung, das die Ausführung von Server-Funktionen des Policy Director Credentials Acquisition Service, wie beispielsweise Systemstart, Server-Registrierung und Signalverarbeitung, ermöglicht. Der Entwickler des Policy Director Credentials Acquisition Service ist verantwortlich für die Erweiterung des Credentials Acquisition Service-Gerüsts, um die Identitätszuordnungsfunktionen ausführen zu können, die von der jeweiligen Anwendung benötigt werden.

Weitere Informationen über die Komponenten von Policy Director befinden sich im Handbuch *Policy Director Administration Guide*.

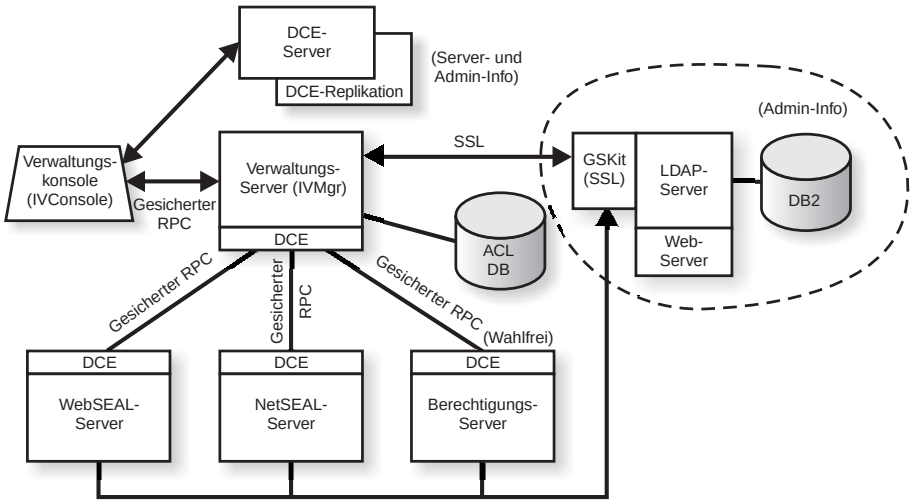
Funktionsweise von Policy Director

Die folgenden Abschnitte zeigen vier Szenarios, die die typischen Verwendungen von Policy Director demonstrieren:

- Ein Administrator, der die Verwaltungskonsole verwendet
- Ein Benutzer, der von einem Web-Browser aus auf geschützte Web-Ressourcen zugreift
- Ein Benutzer, der mit Hilfe eines NetSEAT-Clients auf einen geschützten TCP/IP-Server zugreift
- Ein Benutzer, der auf einen geschützten Server Dritter zugreift

Verwaltung mit Hilfe der Verwaltungskonsole

Die folgende Abbildung zeigt den Datenfluß, wenn ein Administrator die Verwaltungskonsole verwendet, um Policy Director zu verwalten. Die LDAP-Komponenten, die innerhalb der gestrichelten Linie gezeigt werden, sind nur erforderlich, wenn LDAP als Benutzerregistrierungsdatenbank verwendet wird.



Ein Administrator an der Verwaltungskonsole authentifiziert sich für die gesicherte Domäne und empfängt Berechtigungen.

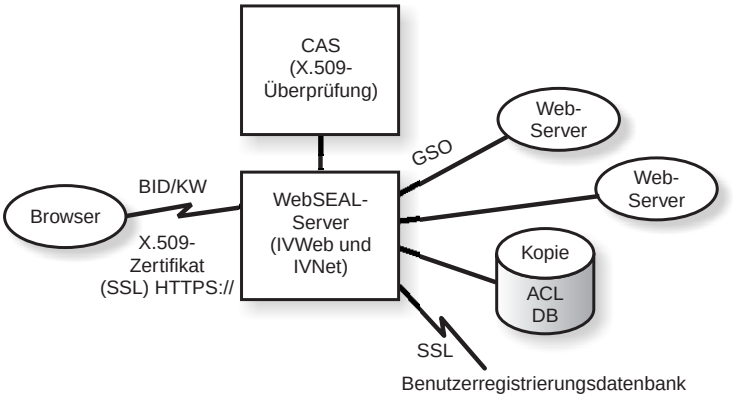
Wenn der Administrator Benutzer oder Gruppen von der Verwaltungskonsole aus verwaltet, sendet die Verwaltungskonsole Anforderungen über einen gesicherten RPC (Remote Procedure Call - Fernprozeduraufruf) an den Verwaltungs-Server.

Der Verwaltungs-Server sendet die entsprechenden Änderungen über eine SSL-Verbindung, die zuvor unter Verwendung des registrierten Namens und des Kennworts des Verwaltungs-Servers hergestellt wurde, an den LDAP-Server.

Wenn der Administrator eine Zugriffssteuerungsliste (Access Control List = ACL) hinzufügt, ändert oder anwendet, sendet die Verwaltungskonsole die Daten über einen gesicherten RPC an den Verwaltungs-Server. Der Verwaltungs-Server speichert dann die Änderungen in der lokalen Kopie der ACL-Datenbank. Wird die erforderliche ACL-Datenbank geändert, benachrichtigt der Verwaltungs-Server alle anderen Server über einen gesicherten RPC, daß die ACL-Datenbank geändert wurde. Die WebSEAL-, NetSEAL- und Berechtigungs-Server überprüfen ebenfalls zusammen mit dem Verwaltungs-Server in regelmäßigen Abständen die ACL-Datenbank auf Aktualisierungen.

Benutzer, der von einem Web-Browser aus auf geschützte Web-Ressourcen zugreift

Die folgende Abbildung zeigt den Datenfluß, wenn ein Benutzer von einem Web-Browser aus auf geschützte Web-Ressourcen zugreift.



Versucht der Benutzer, auf eine geschützte Web-Seite zuzugreifen, stellt der SSL-aktivierte Browser eine Verbindung zum WebSEAL-Server her. Ist WebSEAL für eine Authentifizierung konfiguriert, die auf einem Client-Zertifikat basiert, fordert WebSEAL ein X.509-Zertifikat von dem Browser an. Nachdem WebSEAL das Zertifikat von dem Browser empfangen hat, wird das Zertifikat an den CAS-Server übergeben. CAS versucht, das empfangene Zertifikat einer Benutzeridentifikation zuzuordnen, die von Policy Director erkannt wird. Innerhalb der CAS-Konfigurationsdatei kann der Policy Director-Administrator eine Tabelle erstellen, mit der der registrierte Name (DN = Distinguished Name) eines Zertifikats dem registrierten Namen (DN) eines Policy Director-Benutzers zugeordnet wird. Wird CAS von WebSEAL mit einem Zertifikat aufgerufen, wird zuerst der registrierte Name aus dem Zertifikat extrahiert und die Tabelle nach einer Übereinstimmung durchsucht. Wird eine Übereinstimmung gefunden, gibt CAS den zugehörigen registrierten Namen des Policy Director-Benutzers an WebSEAL zurück. WebSEAL verwendet dann diesen registrierten Namen zur Identifizierung des Policy Director-Benutzers. Wird keine Übereinstimmung gefunden, gibt CAS den registrierten Namen aus dem Zertifikat an WebSEAL zurück. In diesem Fall wird der registrierte Name in dem Zertifikat zur Identifizierung des Policy Director-Benutzers verwendet. Der WebSEAL-Server verwendet den zurückgegebenen registrierten Namen, um die Berechtigung des Benutzers abzurufen.

Weitere Informationen über X.509-Zertifikate können über folgende Web-Adresse angefordert werden:

`http://www.ietf.org`

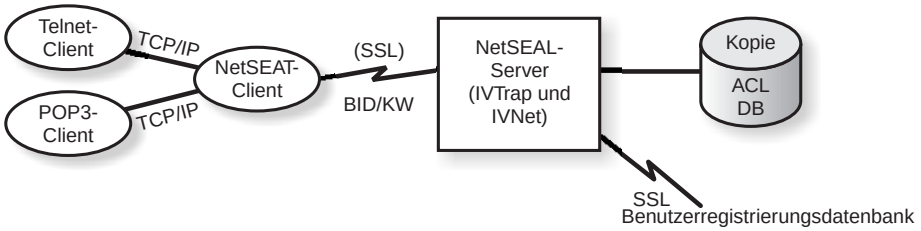
Nachdem WebSEAL die Authentifizierung des Benutzers erfolgreich abgeschlossen hat, bestimmt WebSEAL anhand der lokalen Replikation der ACL-Datenbank, ob der Benutzer für den Zugriff auf das Web-Objekt in der angeforderten Art berechtigt ist.

Ist die Verbindung zwischen dem WebSEAL-Server und dem Back-End-Server, der die Web-Ressource enthält, auf die zugegriffen wird, eine GSO-Junction (GSO = Global Sign-On), sucht WebSEAL nach der GSO-Berechtigung für diese Junction in LDAP und übergibt den Benutzernamen und das Kennwort an den Web-Server.

Informationen über die Verwaltung von GSO-Ressourcen und GSO-Ressourcengruppen befinden sich in den Informationen zur Verwaltungskonsole im Handbuch *Policy Director Administration Guide*.

Benutzer, der mit Hilfe eines NetSEAT-Clients auf einen geschützten TCP/IP-Server zugreift

Die folgende Abbildung zeigt den Datenfluß, wenn ein Benutzer unter Verwendung eines NetSEAT-Clients auf einen geschützten TCP/IP-Server zugreift.



Der Benutzer an dem Telnet-Client stellt eine Verbindung zu einem geschützten NetSEAL-Server her. Dieser erkennt, daß der Benutzer den Zugriff anfordert. NetSEAL fragt nach dem Benutzernamen und nach dem Kennwort und prüft die Identität des Benutzers, indem die Benutzerinformationen zur Verfügung gestellt und mit dem Wert verglichen werden, der in der Benutzerregistrierungsdatenbank gespeichert ist.

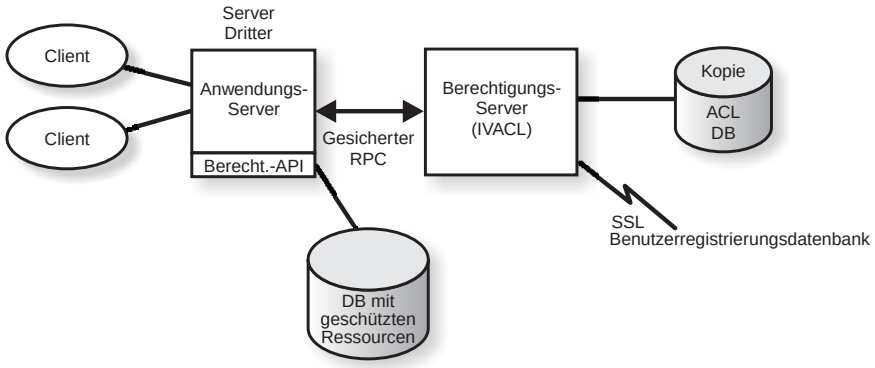
NetSEAL bestätigt, daß der Benutzer über den angegebenen Port auf den Computer zugreifen kann.

NetSEAT leitet Anforderungen auf transparente Weise an gesicherte Policy Director-Server um. Dabei werden die Informationen durch einen gesicherten SSL-Tunnel gesendet. NetSEAT verwendet dessen Konfigurationsdaten für die Erkennung von Anforderungen an einen gesicherten Server von generischen TCP/IP-Anwendungen, wie beispielsweise Telnet, POP3 oder HTTP. NetSEAT verwendet eine Basisauthentifizierung über SSL, um die Identität und Berechtigung des NetSEAT-Benutzers zu definieren. Nachdem die Berechtigung definiert wurde, wird die angeforderte Transaktion gemäß den gültigen Sicherheitseinstellungen vom gesicherten SSL verschlüsselt und ausgeführt.

Fordert ein Web-Browser beispielsweise den Zugriff auf einen Service oder eine Ressource an, der bzw. die durch den Sicherheitsmanager von Policy Director gesichert ist, fängt NetSEAT auf transparente Weise die Anforderung ab und leitet sie an den entsprechenden Server weiter. Ist dies die erste Anforderung an Policy Director und erfordert sie eine Authentifizierung, wird dem Benutzer von NetSEAT ein Anmeldedialogfenster angezeigt. Nach der Authentifizierung des Benutzers ordnet Policy Director die entsprechende Berechtigung auf transparente Weise jeder zukünftigen Anforderung von Informationen zu. Dieser Prozeß ermöglicht eine Umgebung mit Einzelanmeldung für alle Winsock-Anwendungen, die von Policy Director verwaltet werden. Darüber hinaus verwendet Policy Director diese Berechtigung, um zu bestimmen, ob der Benutzer auf die angeforderte geschützte Policy Director-Ressource zugreifen darf.

Benutzer, der auf einen geschützten Server Dritter zugreift

Die folgende Abbildung zeigt den Datenfluß, wenn ein Benutzer auf einen geschützten Server Dritter zugreift.



Versucht ein Client, auf geschützte Daten auf einem geschützten Server Dritter zuzugreifen, authentifiziert der Server Dritter den Benutzer und gleicht ihn mit einem Policy Director-Benutzer ab. Der Anwendungs-Server übergibt die Policy Director-Benutzerinformationen an den Berechtigungs-Server, der eine Verbindung zu LDAP herstellt (oder zu einem anderen Produkt, wie beispielsweise DCE, das für die Benutzerregistrierungsdatenbank verwendet wird) und die Berechtigung des Benutzers abruft. Der Anwendungs-Server übergibt dann die Berechtigung, den Namen des Objekts, auf das der Benutzer zugreifen will, und die Operation, die der Benutzer ausführen will, an den Berechtigungs-Server, der zurückmeldet, ob die Operation erlaubt werden soll. Der Anwendungs-Server erteilt oder verweigert dann den Zugriff.

Inhalt des Policy Director-Pakets

Das Produkt IBM SecureWay Policy Director, Version 3.0, wird auf fünf CDs geliefert. Bezeichnung und Inhalt der CDs werden in der folgenden Tabelle gezeigt.

Bezeichnung der CD	Inhalt
IBM SecureWay Policy Director Version 3.0	• IBM Policy Director Version 3.0
IBM SecureWay Policy Director Security Services	• IBM DCE für AIX Version 2.2 • IBM DCE für Windows NT Version 2.2 • Transarc DCE für Solaris Version 2.0
IBM SecureWay Directory Version 3.1.1 für AIX	• IBM SecureWay Directory Version 3.1.1 • IBM DB2 Version 5.2 mit Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit Version 3.0.1 (GSKit)
IBM SecureWay Directory Version 3.1.1 für NT	• IBM SecureWay Directory Version 3.1.1 • IBM DB2 Version 5.2 mit Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit Version 3.0.1 (GSKit)
IBM SecureWay Directory Version 3.1.1 für Solaris	• IBM SecureWay Directory Version 3.1.1 • IBM DB2 Version 5.2 mit Fix Pack 8 • IBM Global Security Kit SSL Runtime Toolkit Version 3.0.1 (GSKit)

Systemvoraussetzungen

Ihre Betriebsumgebung muß die Software- und Hardwarevoraussetzungen erfüllen, die in den folgenden Abschnitten beschrieben werden. Die neuesten Informationen über Systemvoraussetzungen sind in der Policy Director-Informationsdatei enthalten. Die Informationsdatei enthält aktuelle Informationen, die die Informationen in den Produktveröffentlichungen ersetzen.

Soll die neueste Informationsdatei angefordert werden, auf die Bibliotheksseite der IBM SecureWay Policy Director Web-Site zugreifen.

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

Bevor Sie die Policy Director DCE-, LDAP-, NetSEAT- und Server-Komponenten installieren, stellen Sie sicher, daß Sie über die erforderliche Hardware und Software verfügen, die in den folgenden Abschnitten aufgelistet ist.

Hardwarevoraussetzungen

Speicherbelegung, Pufferverwaltung und Cache-Verwaltung sowie Steuerstrukturen sind skalierbar. Die zugrundeliegenden Anforderungen Ihres Basisbetriebssystems, die Anforderungen der vorausgesetzten DCE- und LDAP-Clients und die Anforderungen Ihrer Client-Anwendungen bestimmen jedoch die Mindestanforderungen bezüglich Plattenspeicherplatz und Hauptspeicher für Ihre Konfiguration.

Die Hardwarevoraussetzungen für den Policy Director-Server sind:

Plattform	Mindest-plattenspei-cherplatz	Mindest-hauptspei-cher
Windows NT-Server mit Intel- oder Intel-kompatiblem 80486-Prozessor mit 133 MHz oder höher	16 MB	64 MB
AIX-Server mit Hardware, auf der AIX 4.3.1 ausgeführt werden kann	16 MB	64 MB
Solaris-Server mit Hardware, auf der Solaris 2.6 ausgeführt werden kann	16 MB	64 MB

Die Hardwarevoraussetzungen für den Policy Director-Client sind:

Plattform	Mindest-plattenspei-cherplatz	Mindest-hauptspei-cher
Windows NT-Client mit Intel- oder Intel-kompatiblem 80486-Prozessor mit 133 MHz oder höher	16 MB	32 MB
AIX-Server mit Hardware, auf der AIX 4.3.1 ausgeführt werden kann	16 MB	32 MB
Solaris-Server mit Hardware, auf der Solaris 2.6 ausgeführt werden kann	16 MB	24 MB

Softwarevoraussetzungen

Stellen Sie während der Planung Ihrer Policy Director-Installation sicher, daß Sie über die in den folgenden Abschnitten aufgelisteten korrekten Versionen der Betriebssysteme verfügen und die anderen genannten Softwarevoraussetzungen erfüllen. Nachfolgend sind die Betriebssystemvoraussetzungen für die Policy Director-Server, den NetSEAT-Client und die Verwaltungskonsole aufgeführt:

Policy Director-Server

Die Policy Director-Server können unter den folgenden Betriebssystemen installiert werden:

- Windows NT Server Version 4.0 mit Service Pack 4 oder höher
- AIX Version 4.3.1 oder höher
- Sun Solaris Version 2.6

NetSEAT-Clients

Policy Director NetSEAT-Clients können unter den folgenden Betriebssystemen installiert werden:

- Windows NT Version 4.0 mit Service Pack 4 oder höher
- Windows 98
- Windows 95

Verwaltungskonsole

Die Policy Director-Verwaltungskonsole kann unter den folgenden Betriebssystemen installiert werden:

- Windows NT Server, Version 4.0, mit Service Pack 4 oder höher
- Windows NT, Windows 95 oder Windows 98
- AIX Version 4.3.1 oder höher, einschließlich Java Runtime 1.1.6 oder höher
- Sun Solaris Version 2.6

Andere Softwarevoraussetzungen

Policy Director erfordert einen DCE-Server und bei Verwendung von LDAP als Benutzerregistrierungsdatenbank einen LDAP-Server. Ein Server (entweder LDAP oder DCE) muß sich auf mindestens einem Computer in der gesicherten Domäne befinden. Die DCE- und LDAP-Clients und -Server werden als Teil des Policy Director-Produkts zur Verfügung gestellt. Sie können diese installieren, bevor Sie Policy Director installieren, oder Sie können eine vorhandene Installation von DCE und LDAP verwenden, die sich auf der korrekten Stufe befindet.

Windows NT und AIX

Auf den Plattformen Windows NT und AIX erfordern Policy Director-Server die folgende Software:

- IBM DCE für Windows NT Version 2.2 oder höher für Windows NT-Server oder IBM DCE für AIX Version 2.2 oder höher für AIX-Server
- IBM SecureWay Directory Version 3.1.1 (LDAP), das DB2& Version 5.2, Fix Pack 7 enthält. LDAP ist nur erforderlich, wenn LDAP als Benutzerregistrierungsdatenbank verwendet wird.
- Secure Sockets Layer (SSL) Version 3.0 oder höher.
- Policy Director Credentials Acquisition Service (CAS) und WebSEAL erfordern einen der folgenden Web-Browser:
  - Microsoft Internet Explorer Version 4 oder höher
  - Netscape Communicator Version 4.5 oder höher
  - Netscape Navigator Version 4.5 oder höher
- Für Policy Director-Clients, die unter Windows 95 ausgeführt werden, muß Winsock Version 2.0 oder höher verfügbar sein.

Solaris

Auf der Solaris-Plattform erfordern Policy Director-Server die folgende Software:

- Transarc DCE Version 2.0.
- IBM SecureWay Directory (LDAP) Version 3.1.1, das DB2 Version 5.2, Fix Pack 8 enthält. LDAP ist nur erforderlich, wenn LDAP als Benutzerregistrierungsdatenbank verwendet wird.
- Secure Sockets Layer Version 3.0 oder höher.
- Policy Director CAS und WebSEAL erfordern einen der folgenden Web-Browser:
  - Microsoft Internet Explorer Version 4 oder höher
  - Netscape Communicator Version 4.5 oder höher
  - Netscape Navigator Version 4.5 oder höher

Planung für Policy Director

Die folgenden Abschnitte stellen die für die Vorbereitung und Planung der Installation und Konfiguration von Policy Director erforderlichen Informationen zur Verfügung. Lesen Sie „Erläuterungen zu Policy Director“ auf Seite 1, und entscheiden Sie, welche Komponenten von Policy Director benötigt werden, bevor Sie Ihre Installation planen.

Allgemeine Konfigurationen

Die in diesem Abschnitt enthaltenen Konfigurationen können bei der Festlegung der geeigneten Konfiguration für Ihr Netz helfen. Verwenden Sie die Tabelle in „Komponenten, die für allgemeine Konfigurationen erforderlich sind“ auf Seite 20, um die Komponenten zu bestimmen, die für Ihre Konfiguration benötigt werden. Wählen Sie dann diese Komponenten während der Policy Director-Installation aus. Beachten Sie, daß WebSEAL und NetSEAL auf jedem Computer installiert werden können. Einige allgemeine Policy Director-Komponentenkonfigurationen werden in der folgenden Liste gezeigt:

Nur Verwaltungs-Server
: Ein Server, der das einzige Exemplar des Verwaltungs-Servers für die gesicherte Domäne ausführt. In diesem Szenario befindet sich der Verwaltungs-Server auf seinem eigenen System. Der Verwaltungs-Server verwaltet die Hauptberechtigungsdatenbank für die gesicherte Domäne, repliziert diese Datenbank in der gesamten gesicherten Domäne und verwaltet Standortinformationen über andere Policy Director-Server in der gesicherten Domäne.

Sicherheitsmanager mit WebSEAL-Server
: Zwei Komponenten bilden WebSEAL—der Sicherheitsmanager (IVNet) und WebSEAL (IVWeb). Ein WebSEAL-Server schützt einen Web-Bereich. WebSEAL unterstützt Back-End-Server für Hochverfügbarkeit und Fehlertoleranz über *intelligente Junctions* oder Junctions.

Sicherheitsmanager mit NetSEAL-Server
: Zwei Komponenten bilden NetSEAL—der Sicherheitsmanager (IVNet) und NetSEAL (IVTrap). Ein NetSEAL-Server sichert ein VPN (Virtual Private Network) und stellt eine Zugriffssteuerung für übernommene Netzservices und Netzservices Dritter zur Verfügung.

Sicherheitsmanager mit WebSEAL- und NetSEAL-Server
: Eine Kombination aus WebSEAL- und NetSEAL-Server.

Berechtigungs-Server
: Ein Server, der unter Verwendung der Policy Director-Berechtigungs-API den Zugriff auf den Policy Director-Berechtigungsservice für Anwendungen Dritter zur Verfügung stellt.

Berechtigungs-Server und ADK
Ein Server, der eine Entwicklungsumgebung für Entwickler zur Verfügung stellt, die Anwendungen Dritter erstellen möchten, die die Policy Director-Berechtigungs-API für den Aufruf des Berechtigungsservices verwenden.

Verwaltungskonsole
Eine Java-gestützte grafische Anwendung, mit der Sicherheitsmaßnahmen für die gesicherte Policy Director-Domäne verwaltet werden. IVBase ist für die Verwaltungskonsole unter Windows nicht erforderlich.

Alle Komponenten
Ein Server, der die kombinierten Services aller oben genannten Konfigurationen zur Verfügung stellt.

Komponenten, die für allgemeine Konfigurationen erforderlich sind

Die Policy Director-Konfigurationen, die in „Allgemeine Konfigurationen“ auf Seite 19 beschrieben werden, sind in der folgenden Tabelle aufgelistet. Die Tabelle zeigt die Komponenten, die für jede Konfiguration installiert werden müssen. Werden die angegebenen Komponenten von links nach rechts gelesen, befinden sie sich in der korrekten Installationsreihenfolge.

Beachten Sie, daß zwei Komponenten sowohl WebSEAL als auch NetSEAL bilden:

WebSEAL Sicherheitsmanager (IVNet) und WebSEAL (IVWeb)

NetSEAL Sicherheitsmanager (IVNet) und NetSEAL (IVTrap)

Anmerkungen zu IVBase:

- IVBase ist für die Verwaltungskonsole unter Windows nicht erforderlich.
- IV.Smit wird mit IV.Base automatisch unter AIX installiert.

Szenarios	Installationspakete							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
Nur einzelnes Exemplar des Verwaltungs-Servers	X	X						
Sicherheitsmanager mit WebSEAL	X	X***	X	X				
Sicherheitsmanager mit NetSEAL	X	X***	X		X			
Sicherheitsmanager mit WebSEAL und NetSEAL	X	X***	X	X	X			

Szenarios	Installationspakete							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
Berechtigungs-Server	X	X***				X		
Berechtigungs-Server und ADK	X	X***				X	X	
Verwaltungskonsole	X							X
Alle Komponenten	X	X***	X	X	X	X	X	X

*** Ist dies der erste oder einzige Computer in der gesicherten Domäne, muß der Verwaltungs-Server (IVMgr) installiert werden. Ist dies ein zusätzlicher Computer in einer vorhandenen gesicherten Domäne mit einem vorhandenen Verwaltungs-Server, darf kein anderer Verwaltungs-Server installiert werden. Es darf nur ein Verwaltungs-Server in einer gesicherten Domäne vorhanden sein.

Informationen, die vor der Installation benötigt werden

Bevor Sie mit der Installation von Policy Director beginnen, notieren Sie die Systeminformationen, die für die Installation der Policy Director-Software erforderlich sind:

Policy Director-Server

- Benutzername für Zellenadministrator (cell_admin)
- Kennwort für Zellenadministrator (cell_admin)
- WebSEAL: HTTP-Port (Standardwert)
- WebSEAL: Stammverzeichnis für Web-Dokument

NetSEAT-Client (nur Windows)

- Zellenname
- Host-Name des Sicherheits-Servers
- Host-Name des Zeit-Servers
- Host-Name des Directory Services Broker

Tunnelmechanismen

Policy Director unterstützt die folgenden Protokolle für die Übertragung verschlüsselter Daten:

- SSL-Tunnelmechanismus (SSL = Secure Sockets Layer)
- GSS-Tunnelmechanismus (GSS = Generic Security Services)

WebSEAL unterstützt Datenintegrität und Datenschutz, die durch den SSL-verschlüsselten Tunnel zur Verfügung gestellt werden. WebSEAL und NetSEAL unterstützen RPCs. Die Verwendung von Integrität und Zeitmarken mit RPC bietet Schutz vor *Wiedergabeangriffen*. Ein Wiedergabeangriff erfolgt, wenn die Daten eines Benutzers abgefangen werden, während sie zwischen dem Client dieses Benutzers und dem Server fließen. Diese Daten werden dann wiederholt oder zu dem Zweck erneut an den Server übergeben, um diesen ersten Benutzer zu imitieren.

SSL-Tunnelmechanismus: Das SSL-Protokoll erlaubt den Austausch von Signalen, um die Kommunikation zwischen zwei Workstations aufzubauen. Dieses Protokoll bietet Sicherheit und Vertraulichkeit im Internet. SSL verwendet allgemeine Schlüssel für die Authentifizierung und geheime Schlüssel für die Verschlüsselung von Daten, die über die SSL-Verbindung übertragen werden.

Aktivieren Sie SSL, wenn die SSL-Tunnelfunktion für Policy Director NetSEAL-Server verwendet wird. Diese Konfiguration wird verwendet, wenn ein NetSEAT-Client als SSL-Client für einen Policy Director NetSEAL-Server dient, der bestimmte Ports sichert (beispielsweise den Port, der von Telnet verwendet wird).

Policy Director WebSEAL unterstützt die SSL-Versionen 2 und 3.

GSS-Tunnelmechanismus: Die GSS-Schnittstelle (GSS API) bietet eine Standardmethode, mit der Anwendungen der Zugriff auf Sicherheitsservices erlaubt werden kann. Der GSS-Tunnelmechanismus wird für gesicherte RPCs verwendet. Aktivieren Sie diese Option, wenn Sie den NetSEAT-Client als Unterstützungsmodul entweder für Policy Director für Microsoft& Windows NT& oder für die Policy Director-Verwaltungskonsole installieren.

Die GSS-Tunnelfunktion stellt Aufrufenden Sicherheitsservices auf generische Art und Weise zur Verfügung. Sie wird von einer Reihe zugrundeliegender Mechanismen und Technologien unterstützt. Sie erlaubt die Übertragbarkeit von Anwendungen auf Quellenebene auf verschiedene Umgebungen. Mit der GSS-Tunnelfunktion kann die Stufe des Schutzes für Datenverkehr gesteuert werden, der unabhängig voneinander in beide Richtungen fließt. Beispielsweise können Daten, die vom Client zum Server fließen, durch Massendatenverschlüsselung vollständig geschützt sein, während Daten, die vom Server zum Client fließen, ungeschützt sein können.

Installationsvoraussetzungen für die gesicherte Domäne

Policy Director ist ein in hohem Maße verteiltes Sicherheitssystem, dessen Komponenten mit verschiedenen Konfigurationen auf einem oder auf mehreren Computern installiert werden können. Die folgende Liste zeigt die Komponenten, die für die gesicherte Domäne installiert werden müssen.

- DCE-Services
- Eine Benutzerregistrierungsdatenbank. (IBM SecureWay Directory ist nur erforderlich, wenn LDAP als Benutzerregistrierungsdatenbank verwendet wird.)
- Policy Director-Server
- Policy Director-Verwaltungskonsole
- Policy Director Authorization ADK

Verwenden Sie eine vorhandene Installation von DCE oder LDAP, stellen Sie sicher, daß sich die vorhandene Installation auf der korrekten Stufe befindet. Der Abschnitt „Andere Softwarevoraussetzungen“ auf Seite 17 enthält die korrekten Stufen. Beachten Sie die folgenden Abhängigkeiten, bevor Sie das Policy Director-Produkt installieren.

Distributed Computing Environment-Services

Jede gesicherte Policy Director-Domäne (DCE-Zelle) erfordert eine vollständige Installation der DCE-Services auf mindestens einem Computer, um die Kommunikation zwischen Policy Director-Servern zu sichern. DCE-Services können sich auf demselben Host wie die Policy Director-Server befinden oder können auf einen fernen Host in dem Netz gestellt werden.

Informationen über die Installation von DCE sind in den Installations- und Verwaltungshandbüchern und über die Ressourcen für die technische Unterstützung für die erforderlichen Plattformen verfügbar. Der Abschnitt „Dokumentation zu IBM Distributed Computing Environment“ auf Seite 90 enthält eine Liste der DCE-Dokumentationen.

Verwenden Sie die folgenden Richtlinien bei der Installation von DCE:

- Wird eine neue gesicherte Policy Director-Domäne auf einem einzelnen Host-System erstellt, führen Sie eine vollständige DCE-Server-Installation durch.
- Befinden sich die DCE-Server auf einem fernen Host, erstellen Sie eine neue gesicherte Domäne, indem Sie Policy Director auf einem lokalen Host installieren.
- Installieren Sie Policy Director für Windows NT in einer vorhandenen gesicherten Policy Director-Domäne, verwenden Sie den NetSEAT-Client, um den Zugriff auf die erforderlichen DCE-Services zur Verfügung zu stellen. Installieren Sie den NetSEAT-Client auf demselben Host wie die Server von Policy Director für Windows NT.

Benutzerregistrierungsdatenbank

Policy Director kann entweder die Benutzerregistrierungsdatenbank von IBM SecureWay Directory (LDAP) oder von DCE als seine Benutzerregistrierungsdatenbank verwenden.

Wird LDAP als Benutzerregistrierungsdatenbank verwendet, müssen Sie einen LDAP-Server installieren und konfigurieren, bevor Sie Policy Director installieren. Außerdem müssen Sie einen LDAP-Client auf jedem Policy Director-Computer installieren.

Das *IBM SecureWay Directory Installations- und Konfigurationshandbuch, Version 3.1.1* enthält Informationen über die LDAP-Installation. Der Abschnitt „Dokumentation zu IBM SecureWay Directory“ auf Seite 91 gibt Auskunft über den Standort dieser LDAP-Dokumentation.

Die im Abschnitt „Dokumentation zu IBM Distributed Computing Environment“ auf Seite 90 aufgelisteten DCE-Produktinformationen enthalten Informationen über die Installation von DCE.

Policy Director-Server

Die folgenden Voraussetzungen gelten für die Installation der Policy Director-Server.

- Um korrekt kommunizieren zu können, benötigen alle Server von Policy Director für Windows NT den Policy Director NetSEAT-Client.
- Für alle Policy Director-Server-Installationen ist die Basiskomponente erforderlich, die automatisch installiert wird.
- Installieren Sie den *ersten* oder *einzigen* Computer in der gesicherten Domäne, müssen Sie den Verwaltungs-Server auf dem Computer installieren.
- Installieren Sie einen *zusätzlichen* Computer in einer vorhandenen gesicherten Domäne, die bereits über einen Verwaltungs-Server verfügt, installieren Sie keinen weiteren Verwaltungs-Server. Es darf nur ein Exemplar des Verwaltungs-Servers in einer gesicherten Domäne vorhanden sein.
- Die Komponenten WebSEAL, NetSEAL und Berechtigungs-Server Dritter sind wahlfrei.
- Der Sicherheitsmanager stellt zusammen mit WebSEAL die WebSEAL HTTP-Server-Komponente und die feinkörnige HTTP-Zugriffssteuerung zur Verfügung. In Verbindung mit NetSEAL stellt der Sicherheitsmanager die grobkörnige NetSEAL TCP/IP-Zugriffssteuerung zur Verfügung.
- Alle Policy Director-Server unter AIX und Solaris erfordern einen vollständigen DCE-Client und bei Verwendung von LDAP als Benutzerregistrierungsdatenbank einen LDAP-Client.

Verwaltungskonsole

Die Verwaltungskonsole erfordert es, daß die gesicherte Domäne und der Verwaltungs-Server installiert und konfiguriert sind. Die Verwaltungskonsole benötigt außerdem einen DCE-Client und, wenn sie sich auf einem Windows-Computer befindet, den NetSEAT-Client.

Authorization ADK

Installieren Sie Policy Director Authorization ADK auf dem Anwendungsentwicklungs-computer. Mit dem Authorization ADK können Anwendungen entwickelt werden, die Benutzern den Zugriff auf geschützte Server Dritter ermöglichen. Der Authorization ADK erfordert die Basiskomponente, die automatisch installiert wird, wenn der Authorization ADK installiert wird.

Für die gesicherte Domäne, in der die Anwendung ausgeführt wird, muß ein Berechtigungs-Server auf mindestens einem Computer installiert sein. In einer typischen Entwicklungsumgebung befindet sich der Berechtigungs-Server auf dem-selben System wie der Authorization ADK.

Übersicht über die schrittweise Installation von Policy Director

Für die Installation von Policy Director sind die folgenden Schritte auszuführen:

1. Ist eine vorherige Version von IBM SecureWay Policy Director installiert und soll die Installation migriert werden, lesen Sie die Migrationsinformationen auf der Policy Director Web-Seite (siehe „Web-Informationen“ auf Seite ix).
2. Stellen Sie sicher, daß Ihr Betriebssystem Policy Director unterstützt.

   Der Abschnitt „Policy Director-Server“ auf Seite 16 enthält Informationen über die unterstützten Betriebssysteme.
3. Bestimmen Sie, welche Server-Komponenten Ihren Anforderungen am besten ent-sprechen und auf welchen Computern diese Komponenten installiert werden sollen.

   Den Abschnitt „Allgemeine Konfigurationen“ auf Seite 19 zu Rate ziehen.
4. Entscheiden Sie, ob die gesicherte Domäne den SSL-Tunnelmechanismus oder den GSS-Tunnelmechanismus verwenden soll.

   Der Abschnitt „Tunnelmechanismen“ auf Seite 22 enthält weitere Informationen.
5. Installieren und konfigurieren Sie eine DCE-Infrastruktur, wenn keine vorhanden ist.

   Der Abschnitt „Distributed Computing Environment-Services“ auf Seite 23 gibt eine Übersicht über die erforderlichen DCE-Services.

6. Entscheiden Sie, ob die gesicherte Domäne eine LDAP-Benutzerregistrierungsdatenbank oder eine DCE-Benutzerregistrierungsdatenbank verwenden soll. Soll IBM SecureWay Directory (LDAP) als Benutzerregistrierungsdatenbank verwendet werden und wird kein vorhandenes LDAP verwendet, installieren und konfigurieren Sie LDAP.

   „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29, enthält Anweisungen für die Installation von LDAP.

7. Installieren Sie die DCE- und LDAP-Clients auf den Computern, die für die Policy Director-Server verwendet werden sollen.

   Die im Abschnitt „Dokumentation zu IBM Distributed Computing Environment“ auf Seite 90 aufgelisteten DCE-Produktinformationen enthalten Informationen über die Installation von DCE.

8. Installieren Sie die Policy Director-Server-Komponenten.

   Das Installationskapitel für das verwendete Betriebssystem enthält weitere Informationen. Verwenden Sie eines der folgenden Kapitel:

   - „Installation von Policy Director für Windows“ auf Seite 45
   - „Installation von Policy Director für AIX“ auf Seite 59
   - „Installation von Policy Director für Solaris“ auf Seite 75

9. Konfigurieren Sie den Policy Director Credentials Acquisition Service (CAS), wenn Policy Director CAS für die Client-Zertifikatsauthentifizierung verwendet werden soll.

   Der Abschnitt „Credentials Acquisition Service konfigurieren“ auf Seite 27 enthält Informationen über Policy Director CAS.

10. Installieren Sie die Verwaltungskonsole.

    Das Installationskapitel für das verwendete Betriebssystem enthält weitere Informationen. Lesen Sie einen der folgenden Abschnitte:

    - Für Windows NT den Abschnitt „Verwaltungskonsole unter Windows installieren“ auf Seite 54 lesen.
    - Für AIX den Abschnitt „Verwaltungskonsole installieren“ auf Seite 72 lesen, wenn die DCE-Benutzerregistrierungsdatenbank verwendet wird, oder den Abschnitt „Verwaltungskonsole konfigurieren und starten“ auf Seite 63 lesen, wenn die LDAP-Benutzerregistrierungsdatenbank verwendet wird.
    - Für Solaris den Abschnitt „Verwaltungskonsole installieren“ auf Seite 87 lesen.

Policy Director erneut installieren

Muß ein Paket erneut installiert werden, müssen Sie zuerst das vorhandene Paket entfernen und dann das gewünschte Paket erneut installieren. Der Abschnitt „Policy Director entfernen“ auf Seite 73 enthält Anweisungen.

Credentials Acquisition Service konfigurieren

Der Policy Director Credentials Acquisition Service (CAS) ist eine anpaßbare Komponente von Policy Director, mit der Sie die Standardauthentifizierungsmechanismen erweitern können, die von WebSEAL unterstützt werden.

Policy Director CAS wird automatisch installiert. Möchten Sie Policy Director CAS als Ihren Credentials Acquisition Service verwenden, müssen Sie CAS konfigurieren. Die Kapitel 2 und 13 im Handbuch *Policy Director Administration Guide* enthalten Erläuterungen zu Policy Director CAS und Informationen zur Konfiguration von CAS.

Installation und Konfiguration von IBM SecureWay Directory

Soll eine DCE-Benutzerregistrierungsdatenbank verwendet werden, können Sie dieses Kapitel über die Installation und Konfiguration von IBM SecureWay Directory (LDAP) überspringen.

Während der Installation von Policy Director werden Sie aufgefordert, entweder eine LDAP-Benutzerregistrierungsdatenbank oder eine DCE-Benutzerregistrierungsdatenbank auszuwählen.

- Wählen Sie LDAP aus, müssen Sie einen IBM SecureWay Directory Version 3.1.1 (LDAP) Client SDK und Server installieren und dann den LDAP-Server konfigurieren, bevor Sie Policy Director installieren.
- Verwenden Sie SSL für den Zugriff auf den LDAP-Server, muß auch der LDAP-Client konfiguriert werden.

LDAP-Server und -Client installieren

Policy Director erfordert einen LDAP-Server und -Client, wenn Sie LDAP als Benutzerregistrierungsdatenbank verwenden.

Ein LDAP-Server muß sich auf mindestens einem Computer in der gesicherten Domäne befinden. Der LDAP-Client und -Server werden als Teil des Policy Director-Produkts zur Verfügung gestellt. Sie müssen den Client und Server installieren, bevor Sie Policy Director installieren, oder Sie können eine vorhandene Installation von LDAP verwenden, die sich auf der korrekten Stufe befindet.

Während der Installation von LDAP wählen Sie **SecureWay Directory und Client SDK** zum Installieren aus.

Weitere Informationen über die Installation und Konfiguration von LDAP befinden sich im *IBM SecureWay Directory Installations- und Konfigurationshandbuch, Version 3.1.1*. Für alle unterstützten Betriebssysteme ist eine separate Version dieses Handbuchs in HTML-Format auf der entsprechenden CD vorhanden. Der Abschnitt „Dokumentation zu IBM SecureWay Directory“ auf Seite 91 enthält Informationen über den Zugriff auf die Dokumentation.

Nur den LDAP-Client installieren

Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, müssen Sie den LDAP-Client auf jedem System installieren, auf dem Policy Director ausgeführt wird. Der LDAP-Client wird als Teil des Policy Director-Produkts zur Verfügung gestellt. Installieren Sie den LDAP-Client, bevor Sie Policy Director installieren.

Wählen Sie während der Installation von LDAP nur **SecureWay Client SDK** aus, wenn Sie bereits über eine vorhandene Installation des LDAP-Servers verfügen, der mit der korrekten Stufe installiert und für Policy Director konfiguriert ist.

LDAP-Server konfigurieren

Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, müssen Sie den LDAP-Server konfigurieren, bevor Sie den ersten Policy Director-Server installieren. Nach der Konfiguration des LDAP-Servers für das erste Policy Director-System müssen Sie den LDAP-Server nicht neu konfigurieren, wenn Sie zusätzliche Policy Director-Server hinzufügen.

Wurde während der LDAP-Server-Konfiguration der SSL-Zugriff auf den LDAP-Server aktiviert, müssen Sie ein Client/Server-Schlüsseldateipaar auf jeden zusätzlichen Computer kopieren, der den SSL-Zugriff verwendet. Der Abschnitt „SSL-Zugriff aktivieren (wahlfrei)“ auf Seite 33 enthält weitere Informationen.

Zum Konfigurieren des LDAP-Servers müssen Sie die Konfigurationsschritte in der folgenden Liste nur einmal für jede gesicherte Domäne ausführen:

1. Fügen Sie die erforderlichen Suffixe hinzu. Der Abschnitt „Suffixe hinzufügen“ enthält Anweisungen.
2. Installieren Sie Sicherheitsschemaobjekte und -attribute. Siehe „Sicherheitsschemaobjekte und -attribute installieren“ auf Seite 31.
3. Aktivieren Sie die LDAP-Zugriffssteuerung. Der Abschnitt „LDAP-Zugriffssteuerung aktivieren“ auf Seite 42 enthält Anweisungen.
4. Aktivieren Sie den SSL-Zugriff. Der Abschnitt „SSL-Zugriff aktivieren (wahlfrei)“ auf Seite 33 enthält Anweisungen.

Wurde der SSL-Zugriff aktiviert, führen Sie die Schritte in „LDAP-Client für SSL-Zugriff konfigurieren“ auf Seite 39 immer dann aus, wenn Sie einen LDAP-Client (Policy Director-Server) hinzufügen, der SSL für den Zugriff auf den LDAP-Server verwendet.

Anmerkung: LDAP-Administratoren können Einstellungen für die Kennwortverschlüsselung in der LDAP-Datenbank angeben. LDAP erlaubt das Speichern von Kennwörtern im Klartext. Dies kann ein Sicherheitsrisiko darstellen. Die LDAP-Dokumentation enthält Anweisungen zum Setzen von Benutzerkennwortattributen auf die entsprechende Verschlüsselungsebene.

Suffixe hinzufügen

Erstellen Sie in IBM SecureWay Directory ein neues Suffix, indem Sie die folgenden Schritte ausführen:

1. Greifen Sie mit Hilfe eines Web-Browsers auf die Server-Verwaltung für IBM SecureWay Directory unter der folgenden Web-Adresse zu:

   `http://`*`Server-Name`*`/ldap`

   Melden Sie sich über die Web-Schnittstelle als LDAP-Administrator an (beispielsweise `cn=root`).
2. Klicken Sie auf **Suffixe** → **Suffix hinzufügen**.

3. Im Feld **Suffix-DN** müssen Sie folgendes Suffix hinzufügen:

   ```
   secAuthority=Default
   ```

   Das Objekt für `secAuthority=Default` wird während der Konfiguration des Verwaltungs-Servers erstellt.

4. Klicken Sie auf die Schaltfläche **Neues Suffix hinzufügen**.
5. Soll ein anderes Suffix hinzugefügt werden, klicken Sie auf den Link **Suffix hinzufügen**, um zum vorherigen Fenster zurückzukehren.
6. Falls erforderlich, fügen Sie ein Suffix für Ihre Policy Director-Benutzer und GSO-Daten (GSO = Global Sign-On) hinzu. Beispiel:

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

   Sie können die Suffixe wie gewünscht in einer Art und Weise benennen, die Ihrer Installation entspricht. Dabei gibt `o=` den abgekürzten Namen Ihrer Organisation und `c=` das Land an.

   Dieser Schritt erstellt Suffixe für Ihre GSO-Daten und für Ihre Benutzer und Gruppen. Diese Suffixe werden mit dem LDAP-Web-Verwaltungs-Tool erstellt.

7. Klicken Sie auf die Schaltfläche **Neues Suffix hinzufügen**.
8. Wiederholen Sie die Prozedur für jedes neue Suffix, das hinzugefügt werden soll und für Ihre Organisation erforderlich ist.
9. Klicken Sie auf den Link **Server erneut starten** auf der aktuellen Web-Seite des LDAP-Verwaltungs-Tools, um den LDAP-Server erneut zu starten, wenn das Hinzufügen der Suffixe beendet ist.

Sicherheitsschemaobjekte und -attribute installieren

Policy Director verwendet eine Reihe von LDAP-Objekten und -Attributen, um Benutzerberechtigungen innerhalb des LDAP-Servers zu verwalten.

Bestimmen Sie mit Hilfe des IBM SecureWay Directory Management Tool (DMT), ob die Sicherheitsobjekte und -attribute installiert sind. Installieren Sie diese, wenn sie noch nicht vorhanden sind. DMT wird als Teil des IBM SecureWay Directory-Pakets installiert.

Führen Sie die folgenden Schritte aus, um zu bestimmen, ob die Policy Director-Sicherheitsobjekte und -attribute installiert sind:

1. Starten Sie das Directory Management Tool auf einem LDAP-Client.

   Anmerkung: Empfangen Sie die Nachricht, daß kein Eintrag für das Suffix secAuthority=Default vorhanden ist, können Sie unbesorgt fortfahren. Das Objekt für das Suffix secAuthority=Default wird während der Konfiguration des Verwaltungs-Servers erstellt.

2. Klicken Sie auf **Schema** → **Objektklassen** → **Objektklassen anzeigen**.

3. Überprüfen Sie, ob alle folgenden Policy Director-Objekte und -Attribute vorhanden sind:

   Objektklassen
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser

4. Klicken Sie auf **Schema** → **Attribute** → **Attribute anzeigen**.
5. Überprüfen Sie, ob alle folgenden Policy Director-Objekte und -Attribute vorhanden sind:

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

6. Führen Sie auf der Basis der Ergebnisse in Schritt 3 und Schritt 5 einen der folgenden Schritte aus.
   - Sind alle Objekte vorhanden, ist keine weitere Aktion erforderlich. Mit „SSL-Zugriff aktivieren (wahlfrei)“ auf Seite 33 fortfahren.
   - Sind *einige*, aber nicht alle Objekte vorhanden, mit Schritt 7 fortfahren.
   - Sind *keine* Objekte vorhanden, mit Schritt 8 fortfahren.
7. Werden einige, aber nicht alle Policy Director-Objekte und -Attribute gefunden, entfernen Sie die vorhandenen Policy Director-Objekte und -Attribute. Klicken Sie im DMT auf

   Schema → **Objektklassen** → **Objektklassen löschen** und entfernen Sie die Objektklassen.

   Klicken Sie dann auf **Schema** → **Attribute** → **Attribute löschen** und entfernen Sie die Attribute.
8. Werden keine Policy Director-Objekte und -Attribute gefunden, legen Sie die CD mit *IBM SecureWay Policy Director Version 3.0* ein.

9. Verwenden Sie **ldapmodify** in einer Eingabeaufforderung, um die Schemadatei zu laden. Geben Sie beispielsweise folgendes ein:

   UNIX:

   ```
   ldapmodify -h Host-Name -p 389 -D cn=root -w Kennwort -f /schema/secschema.def
   ```

   Windows:

   ```
   ldapmodify -h Host-Name -p 389 -D cn=root -w Kennwort -f x:\schema\secschema.def
   ```

   Dabei ist *x:* der Laufwerkbuchstabe des Windows-CD-ROM-Laufwerks.

10. Soll Policy Director zur Verwaltung von SecureWay Boundary Server-Benutzern verwendet werden, müssen Sie auch die Objekte und Attribute aus der Policy Director-Schemadatei hinzufügen:

    Geben Sie den Befehl **ldapmodify** in eine Befehlszeile ein, um die Schemadatei zu laden. Geben Sie beispielsweise folgendes ein:

    Windows:

    ```
    ldapmodify -h Host-Name -p 389 -D cn=root -w Kennwort -f x:\schema\puschema.def
    ```

    UNIX:

    ```
    ldapmodify -h Host-Name -p 389 -D cn=root -w Kennwort -f /schema/puschema.def
    ```

    Dabei ist *x:* der Laufwerkbuchstabe des CD-ROM-Laufwerks.

SSL-Zugriff aktivieren (wahlfrei)

Ist kein SSL-Zugriff auf Ihren LDAP-Server erforderlich, können Sie diesen Abschnitt überspringen. Fahren Sie mit „LDAP-Zugriffssteuerung aktivieren“ auf Seite 42 fort.

Ist der SSL-Zugriff für den LDAP-Server erforderlich, fahren Sie mit diesem Abschnitt fort. Diese Prozedur muß nur bei der erstmaligen Definition der SSL-Kommunikation zwischen dem LDAP-Server und dem LDAP-Client ausgeführt werden.

Sie können die Verwendung von SSL wahlweise aktivieren, um die Kommunikation zwischen den Policy Director-Servern und dem LDAP-Server zu schützen.

IBM Global Security Kit (GSKit) SSL Runtime Toolkit Version 3.0.1 wird während der Installation von LDAP installiert. GSKit stellt zwei Versionen eines Key Management Tools zur Verfügung—die eine Version ist eine Version mit Fensterfunktion **(ikmguiw)** und die andere Version ist eine Version ohne Fensterfunktion **(ikmgui)**. Sie können beide Versionen verwenden, wenn **ikmguiw** in den folgenden Prozeduren aufgerufen wird. Vollständige Anweisungen zur Verwendung dieses Tools befinden sich in der LDAP-Dokumentation. Siehe „Dokumentation zu IBM SecureWay Directory“ auf Seite 91.

Sie können auch diese abgekürzten Prozeduren verwenden, um speziell Policy Director für den SSL-Zugriff zu aktivieren.

Datenbankschlüsseldatei und Zertifikat erstellen

Zum Aktivieren der SSL-Unterstützung auf dem LDAP-Server muß der Server über ein Zertifikat verfügen, das den Server identifiziert und das vom Server als *persönliches Zertifikat* verwendet werden kann. Dieses persönliche Zertifikat ist das Zertifikat, das der Server an den Client sendet, um dem Client die Authentifizierung des Servers zu erlauben. Die Zertifikate und das allgemeine/private Schlüsselpaar werden in einer Datenbankschlüsseldatei gespeichert. Ein Kunde erwirbt normalerweise ein *unterschriebenes Zertifikat* von einer Zertifizierungsinstanz, wie beispielsweise VeriSign.

Sie können jedoch auch ein *selbstunterschriebenes* Zertifikat verwenden. Bei Verwendung eines selbstunterschriebenen Zertifikats wird die Maschine, auf der das Zertifikat generiert wird, zur Zertifizierungsinstanz.

Verwenden Sie das Key Management Tool des GSKit (**ikmguiw**) zur Erstellung der Datenbankschlüsseldatei und des Zertifikats. Gehen Sie wie folgt vor, um die Datenbankschlüsseldatei und das Zertifikat (selbstunterschrieben oder unterschrieben) zu erstellen:

1. Stellen Sie sicher, daß IBM Global Security Kit (GSKit) SSL Runtime Toolkit Version 3.0.1 und das Java-gestützte Key Management Tool sowohl auf dem LDAP-Server als auch auf allen LDAP-Clients installiert sind, die SSL verwenden.

   Windows: `C:\Programmdateien\IBM\GSK\bin\ikmguiw.exe`

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

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

2. Starten Sie das IBM Key Management Tool (**ikmguiw**).
3. Klicken Sie auf **Key Database File** → **New**.
4. Stellen Sie sicher, daß die **CMS key database file** die ausgewählte Datenbankschlüsselart ist.
5. Geben Sie Informationen in das Feld **File Name** und in das Feld **Location** ein, um den Speicherort der Datenbankschlüsseldatei anzugeben. Die Erweiterung einer Datenbankschlüsseldatei lautet *.kdb*.
6. Klicken Sie auf **OK**.
7. Geben Sie das Kennwort für die Datenbankschlüsseldatei ein und bestätigen Sie das Kennwort.

   Sie dürfen dieses Kennwort nicht vergessen, da es erforderlich ist, wenn die Datenbankschlüsseldatei bearbeitet wird.
8. Akzeptieren Sie die Standardverfallszeit oder ändern Sie die Standardverfallszeit entsprechend den Anforderungen Ihrer Organisation.
9. Soll das Kennwort verdeckt und in einer Stash-Datei gespeichert werden, klicken Sie auf **Stash the password to a file**.

Eine Stash-Datei kann von einigen Anwendungen verwendet werden. Mit ihr muß die Anwendung das Kennwort nicht kennen, um die Datenbankschlüsseldatei verwenden zu können. Die Stash-Datei hat dieselbe Position und denselben Namen wie die Datenbankschlüsseldatei. Sie hat die Erweiterung *.sth*.

10. Klicken Sie auf **OK**.

Damit ist die Erstellung der Datenbankschlüsseldatei abgeschlossen. Es gibt eine Reihe von Standardunterzeichnerzertifikaten (Signer certificates). Diese Unterzeichnerzertifikate sind die Standardzertifizierungsinstanzen, die erkannt werden.

Persönliches Zertifikat erstellen

Soll ein Zertifikat von einer Zertifizierungsinstanz (wie beispielsweise VeriSign) verwendet werden, müssen Sie das Zertifikat von der Zertifizierungsinstanz anfordern und dann in die Datenbankschlüsseldatei stellen. Führen Sie die Schritte unter „Zertifikat empfangen“ aus.

Zertifikat empfangen: Wird anstelle eines selbstunterschriebenen Zertifikats ein Zertifikat von einer Zertifizierungsinstanz (wie beispielsweise VeriSign) verwendet, führen Sie die folgenden Schritte aus:

1. Verwenden Sie **ikmguiw**, um ein Zertifikat von einer Zertifizierungsinstanz anzufordern, und stellen Sie dann das neue Zertifikat in Ihre Datenbankschlüsseldatei.
2. Klicken Sie auf den Abschnitt **Personal Certificate Requests** der Datenbankschlüsseldatei.
3. Klicken Sie auf **New**.
4. Geben Sie alle Informationen ein, um eine Anforderung zu erstellen, die an die Zertifizierungsinstanz gesendet werden kann.
5. Klicken Sie auf **OK**.
6. Nachdem die Zertifizierungsinstanz das Zertifikat zurückgegeben hat, können Sie das Zertifikat in Ihrer Datenbankschlüsseldatei installieren, indem Sie auf den Abschnitt **Personal Certificates** und dann auf **Receive** klicken.
7. Nachdem das Zertifikat des LDAP-Servers in die Datenbankschlüsseldatei gestellt wurde, können Sie den LDAP-Server konfigurieren, um SSL zu aktivieren.

Wird Ihr Zertifikat noch nicht erkannt, kopieren Sie das Zertifikat der Zertifizierungsinstanz auf die Client-Maschine.

Wird Ihr Zertifikat von einer Zertifikatsinstanz generiert, die bereits erkannt wird (wie beispielsweise VeriSign), ist keine weitere Aktion erforderlich. Fahren Sie mit „LDAP-Server konfigurieren, um SSL zu aktivieren“ auf Seite 37 fort.

Selbstunterschriebenes Zertifikat erstellen: Soll anstelle eines Zertifikats von einer Zertifizierungsinstanz (wie beispielsweise VeriSign) ein selbstunterschriebenes Zertifikat verwendet werden, führen Sie die folgenden Schritte aus.

Gehen Sie wie folgt vor, um ein neues selbstunterschriebenes Zertifikat zu erstellen und das Zertifikat in der Datenbankschlüsseldatei zu speichern:

1. Klicken Sie auf **Create** → **New Self-Signed Certificate**.
2. Geben Sie in das Feld **Key Label** einen Namen ein, den GSKit verwenden kann, um dieses neue Zertifikat in der Schlüsseldatenbank zu identifizieren.

   Beispielsweise kann es sich bei dem Kennsatz um den Maschinennamen des LDAP-Servers handeln.
3. Akzeptieren Sie den Standardwert für das Feld **Version**, der X509 V3 lautet, und für das Feld **Key Size**.
4. Akzeptieren Sie für dieses Zertifikat entweder den Standardmaschinennamen oder geben Sie einen anderen registrierten Namen in das Feld **Common Name** ein.
5. Geben Sie einen Firmennamen in das Feld **Organization** ein.
6. Füllen Sie alle Kanneingabefelder aus oder lassen Sie diese Felder leer.
7. Akzeptieren Sie entweder den Standardwert für das Feld **Country** und den Standardwert 365 für das Feld **Validity Period** oder ändern Sie die Standardwerte entsprechend den Anforderungen Ihrer Organisation.
8. Klicken Sie auf **OK**.

   GSKit generiert ein neues allgemeines/privates Schlüsselpaar und erstellt das Zertifikat.

   Sind mehrere persönliche Zertifikate in der Datenbankschlüsseldatei vorhanden, fragt GSKit, ob dieser Schlüssel als Standardschlüssel in der Datenbank verwendet werden soll. Sie können einen Schlüssel als Standardschlüssel akzeptieren. Das Standardzertifikat wird zur Laufzeit verwendet, wenn kein Kennsatz angegeben wird, um das zu verwendende Zertifikat auszuwählen.

Damit ist die Erstellung des persönlichen Zertifikats des LDAP-Servers abgeschlossen. Das Zertifikat sollte im Abschnitt 'Personal Certificates' (Persönliche Zertifikate) der Datenbankschlüsseldatei erscheinen. Verwenden Sie den mittleren Balken im Key Management Tool, um zwischen den Arten von Zertifikaten zu wählen, die in der Datenbankschlüsseldatei gespeichert sind.

Anschließend müssen Sie das Zertifikat Ihres LDAP-Servers in eine Base64-verschlüsselte ASCII-Datendatei extrahieren.

Selbstunterschriebenes Zertifikat extrahieren

Ist Ihr Zertifikat ein selbstunterschriebenes Zertifikat, müssen Sie das Unterzeichnerzertifikat (Signer Certificate) aus der Datenbankschlüsseldatei extrahieren. Fahren Sie mit dieser Extraktionsprozedur fort.

Diese Extraktion wird verwendet, um die Client-Maschine zu definieren. Haben Sie in „Selbstunterschriebenes Zertifikat erstellen“ auf Seite 36 ein selbstunterschriebenes Zertifikat erstellt, erscheint es auch im Abschnitt `Signer Certificates` (Unterzeichnerzertifikate) der Datenbankschlüsseldatei, da es sich um ein selbstunterschriebenes Zertifikat handelt. Befinden Sie sich im Abschnitt 'Signer Certificates' (Unterzeichnerzertifikate) der Datenbankschlüsseldatei, stellen Sie sicher, daß das neue Zertifikat vorhanden ist.

Gehen Sie wie folgt vor, um das Unterzeichnerzertifikat zu extrahieren:

1. Verwenden Sie **ikmguiw**, um das Zertifikat Ihres LDAP-Servers in eine Base64-verschlüsselte ASCII-Datendatei zu extrahieren. Diese Datei wird in der Prozedur in „LDAP-Client für SSL-Zugriff konfigurieren“ auf Seite 39 verwendet.
2. Heben Sie das selbstunterschriebene Zertifikat hervor, das Sie gerade in „Selbstunterschriebenes Zertifikat erstellen“ auf Seite 36 hinzugefügt haben.
3. Klicken Sie auf **Extract Certificate**.
4. Klicken Sie auf **Base64-encoded ASCII data** als Datentyp.
5. Geben Sie einen Zertifikatsdateinamen für das neu extrahierte Zertifikat ein. Die Erweiterung der Zertifikatsdatei lautet *.arm*.
6. Geben Sie die Position ein, an der das extrahierte Zertifikat gespeichert werden soll.
7. Klicken Sie auf **OK**.
8. Kopieren Sie dieses extrahierte Zertifikat auf die LDAP-Client-Maschine.
9. Sie können den LDAP-Server konfigurieren, um SSL zu aktivieren.

LDAP-Server konfigurieren, um SSL zu aktivieren

Gehen Sie wie folgt vor, um den LDAP-Server zum Aktivieren von SSL zu konfigurieren:

1. Stellen Sie sicher, daß der LDAP-Server installiert und aktiv ist, wenn LDAP als Benutzerregistrierungsdatenbank verwendet werden soll. Vollständige Anweisungen befinden sich in „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29.
2. Verwenden Sie das Web-gestützte LDAP-Verwaltungs-Tool mit der folgenden URL:

   `http://`*`Server-Name`*`/ldap`

   Dabei gibt *Server-Name* den Namen der LDAP-Server-Maschine an.

3. Melden Sie sich als LDAP-Administrator an (beispielsweise cn=root), wenn Sie sich noch nicht angemeldet haben.
4. Klicken Sie auf **Server** → **SSL**.
5. Klicken Sie entweder auf **SSL On** für die SSL- und Nicht-SSL-Aktivierung oder auf **SSL Only** für den SSL-Status, der gesetzt werden soll.
6. Klicken Sie auf **Server Authentication** für die Art der Authentifizierungsmethode.
7. Geben Sie eine Port-Nummer ein oder akzeptieren Sie die Standard-Port-Nummer 636.
8. Geben Sie den in Schritt 5 im Abschnitt 'Datenbankschlüsseldatei und Zertifikat erstellen ' angegebenen Pfad und Namen der Datenbankschlüsseldatei ein.

   Die Erweiterung der Datenbankschlüsseldatei lautet *.kdb*
9. Geben Sie in das Feld **Key Label** den Namen ein, den Sie beim Speichern des Zertifikats des LDAP-Servers in der Datenbankschlüsseldatei zur Identifizierung verwendet haben. Beispielsweise kann es sich bei dem Kennsatz um den Maschinennamen des LDAP-Servers handeln.
10. Geben Sie das Kennwort für die Datenbankschlüsseldatei ein und bestätigen Sie das Kennwort. Sie können das Feld für das Kennwort auch leer lassen, wenn der LDAP-Server die Stash-Datei verwenden soll.
11. Klicken Sie auf **Apply**.
12. Klicken Sie auf den Link **Restart the server**, um den LDAP-Server erneut zu starten und diese Änderung zu aktivieren.

SSL-Zugriff testen: Geben Sie den folgenden Befehl in eine Befehlszeile des LDAP-Servers ein, um zu testen, ob SSL aktiviert wurde:

```
ldapsearch -h Server-Name -Z -K Schlüsseldatei -P Kennwort -b "" -s base \
objectclass=*
```

Der umgekehrte Schrägstrich (\) in diesem Befehl ist nur erforderlich, wenn der Befehl nicht in eine Zeile eingegeben werden kann.

Dabei bedeuten:

Option	Beschreibung
Server-Name	Der DNS-Host-Name des LDAP-Servers.
Schlüsseldatei	Der vollständig qualifizierte Pfadname der generierten Schlüsseldatei.
Kennwort	Das Kennwort der generierten Schlüsseldatei.

Dieser Befehl gibt die LDAP-Basisinformationen zurück, die die Suffixe auf dem LDAP-Server einschließen.

Die SSL-Konfiguration für den Server ist jetzt abgeschlossen. Konfigurieren Sie anschließend den LDAP-Client für den SSL-Zugriff.

LDAP-Client für SSL-Zugriff konfigurieren

Nachdem der LDAP-Server für den SSL-Zugriff konfiguriert wurde, müssen Sie die LDAP-Clients für den SSL-Zugriff konfigurieren.

Datenbankschlüsseldatei erstellen: Stellen Sie sicher, daß GSKit auf dem Client installiert ist, und erstellen Sie dann mit dem IBM Key Management Tool wie in „Datenbankschlüsseldatei und Zertifikat erstellen“ auf Seite 34 beschrieben eine neue Datenbankschlüsseldatei.

Damit der Client den LDAP-Server authentifizieren kann, muß der Client die Zertifizierungsinstanz (den Unterzeichner) erkennen, die das Zertifikat des LDAP-Servers erstellt hat. Verwendet der LDAP-Server ein selbstunterschriebenes Zertifikat, muß es dem Client ermöglicht werden, die Maschine zu erkennen, die das Zertifikat des LDAP-Servers als Trusted Root (Zertifizierungsinstanz) generiert hat.

Unterzeichnerzertifikat hinzufügen: Gehen Sie wie folgt vor, um ein Unterzeichnerzertifikat hinzuzufügen, nachdem die Datenbankschlüsseldatei erstellt wurde:

1. Stellen Sie sicher, daß das Zertifikat, das aus der Datenbankschlüsseldatei im Abschnitt „Selbstunterschriebenes Zertifikat extrahieren“ auf Seite 37 extrahiert wurde, auf die Client-Maschine kopiert wurde. Ist dies nicht der Fall, kopieren Sie jetzt das Zertifikat auf die Client-Maschine.
2. Klicken Sie auf den Abschnitt **Signer Certificates** (Unterzeichnerzertifikate) der CMS-Datenbankschlüsseldatei des Clients.
3. Klicken Sie auf **Add**.
4. Klicken Sie auf **Base64-encoded ASCII data**, um den Datentyp zu definieren.
5. Geben Sie den Dateinamen und die Position des Zertifikats an. Die Erweiterung der Zertifikatsdatei lautet *.arm*.
6. Klicken Sie auf **OK**.
7. Geben Sie einen Kennsatz für das Unterzeichnerzertifikat ein, das hinzugefügt wird. Beispielsweise kann der Maschinenname des LDAP-Servers als Kennsatz verwendet werden.
8. Klicken Sie auf **OK**.

   Das selbstunterschriebene Zertifikat erscheint in der Datenbankschlüsseldatei des Clients als Unterzeichnerzertifikat.

9. Heben Sie das neu hinzugefügte Unterzeichnerzertifikat hervor und klicken Sie auf **View/Edit**.
10. Stellen Sie sicher, daß es als Trusted Root markiert ist. Dies ist der Fall, wenn **Set the certificate as a trust root** ausgewählt ist.

    Wurde das Zertifikat des LDAP-Servers von einer regulären Zertifizierungsinstanz generiert, stellen Sie sicher, daß das Zertifikat der Zertifizierungsinstanz als Unterzeichnerzertifikat aufgelistet und als Trusted Root markiert ist. Ist dies nicht der Fall, fügen Sie das Zertifikat der Zertifizierungsinstanz als Unterzeichnerzertifikat hinzu und markieren Sie es als Trusted Root.

An diesem Punkt sollte der Client in der Lage sein, eine SSL-Sitzung mit dem LDAP-Server aufzubauen.

SSL-Aktivierung testen: Geben Sie den folgenden Befehl in eine Befehlszeile des LDAP-Clients ein, um zu testen, ob SSL aktiviert wurde:

```
ldapsearch -h Server-Name -Z -K Client_Schlüsseldatei -P Kennwort -b "" \
-s base objectclass=*
```

Der umgekehrte Schrägstrich (\) in diesem Befehl ist nur erforderlich, wenn der Befehl nicht in eine Zeile eingegeben werden kann.

Dabei bedeuten:

Option	Beschreibung
Server-Name	Der DNS-Host-Name des LDAP-Servers.
Client_Schlüsseldatei	Der vollständig qualifizierte Pfadname der generierten Schlüsseldatei.
Kennwort	Das Kennwort der generierten Schlüsseldatei.

Dieser Befehl gibt die LDAP-Basisinformationen zurück, die die Suffixe auf dem LDAP-Server einschließen.

Die SSL-Konfiguration ist jetzt abgeschlossen.

LDAP-Server- und -Client-Authentifizierung verwenden (wahlfrei)

Dieser Konfigurationsabschnitt ist wahlfrei:

1. Führen Sie die Prozedur wie in „LDAP-Server konfigurieren, um SSL zu aktivieren“ auf Seite 37 beschrieben aus. Anstelle der Konfiguration des LDAP-Servers für **Server Authentication** wählen Sie jedoch **Server and Client Authentication** aus, um beide Authentifizierungen auszuführen.

   Nachdem der Server sein Zertifikat an den Client gesendet hat und der Server durch den Client authentifiziert wurde, fordert der Server in diesem Fall das Zertifikat des Clients an. Ist der LDAP-Server für beide Authentifizierungen konfiguriert, muß auch für die Client-Maschine ein Zertifikat erstellt werden.

2. Auf der Client-Maschine wird ein Zertifikat für die Client-Maschine wie in den folgenden Prozeduren beschrieben erstellt:
   - „Datenbankschlüsseldatei und Zertifikat erstellen“ auf Seite 34
   - „Selbstunterschriebenes Zertifikat erstellen“ auf Seite 36, wenn das Zertifikat ein selbstunterschriebenes Zertifikat ist, oder „Zertifikat empfangen“ auf Seite 35, wenn das Zertifikat ein Unterzeichnerzertifikat ist.
   - „Selbstunterschriebenes Zertifikat extrahieren“ auf Seite 37
   - „LDAP-Server konfigurieren, um SSL zu aktivieren“ auf Seite 37
3. Nachdem das persönliche Zertifikat des Clients erstellt und der Datenbankschlüsseldatei des Clients hinzugefügt wurde, muß auf dem LDAP-Server die Zertifizierungsinstanz, die dieses Client-Zertifikat erstellt hat, als Unterzeichnerzertifikat (Trusted Root) erkannt werden. Das Zertifikat der Zertifizierungsinstanz wird wie in „Unterzeichnerzertifikat hinzufügen“ auf Seite 39 beschrieben der Datenbankschlüsseldatei des LDAP-Servers hinzugefügt.

SSL-Zugriff testen: Wenn der LDAP-Server die Zertifizierungsinstanz erkennt, die das persönliche Zertifikat des Clients erstellt hat, kann die Konfiguration unter Verwendung des folgenden Befehls getestet werden:

```
ldapsearch -h Server-Name -Z -K Client_Schlüsseldatei -P Kennwort
-N Client_Kennsatz \ -b "" \ -s base objectclass=*
```

Der umgekehrte Schrägstrich (\) in diesem Befehl ist nur erforderlich, wenn der Befehl nicht in eine Zeile eingegeben werden kann.

Dabei bedeuten:

Option	Beschreibung
Server-Name	Der DNS-Host-Name des LDAP-Servers.
Client_Schlüsseldatei	Der vollständig qualifizierte Pfadname der generierten Client-Schlüsseldatei.
Kennwort	Das Kennwort der generierten Schlüsseldatei.
Client_Kennsatz	Der Kennsatz, der dem Schlüssel zugeordnet ist (falls vorhanden). Dieses Feld ist wahlfrei und nur erforderlich, wenn der LDAP-Server sowohl für die Server-Authentifizierung als auch für die Client-Authentifizierung konfiguriert ist.

Dieser Befehl gibt die LDAP-Basisinformationen zurück, die die Suffixe auf dem LDAP-Server einschließen. Beachten Sie, daß der Parameter **-N** den Kennsatz angibt, der angegeben wurde, als das persönliche Zertifikat des Clients zur Datenbankschlüsseldatei des Clients hinzugefügt wurde.

Geben Sie nicht den Kennsatz des Unterzeichnerzertifikats des LDAP-Servers an. Der Parameter **-N** teilt GSKit mit, welches Client-Zertifikat auf Anforderung an den Server gesendet wird. Ist kein Kennsatz angegeben, wird das persönliche Standardzertifikat gesendet, wenn der Server das Zertifikat des Clients anfordert.

Die SSL-Konfiguration ist jetzt abgeschlossen.

LDAP-Zugriffssteuerung aktivieren

Um die Integration der Policy Director-Sicherheit mit der LDAP-Benutzerregistrierungsdatenbank abzuschließen, aktualisieren Sie die LDAP ACLs, die die Benutzerregistrierungsdatenbank steuern. Führen Sie dazu die folgenden Schritte aus:

1. Starten Sie das Directory Management Tool entweder von dem LDAP-Client oder von dem LDAP-Server aus, indem Sie auf **Start** → **Programme** → **IBM SecureWay Directory** → **Directory Management Tool** klicken.
2. Den Server erneut binden:
   a. Klicken Sie auf **Server** → **Erneut binden**.
   b. Klicken Sie auf **Authentifiziert**.
   c. Geben Sie den Benutzer-DN ein (zum Beispiel cn=root).
   d. Geben Sie Ihr Kennwort ein.
   e. Klicken Sie auf **OK**.
3. Klicken Sie auf **OK** oder schließen Sie das Warnungsfenster bei jeder Warnung, die angezeigt wird.

4. Geben Sie der Policy Director-Sicherheitsdämongruppe die vollständige Steuerung für die Suffixe, die Sie unter „Suffixe hinzufügen“ auf Seite 30 erstellt haben.
   a. Klicken Sie auf **Einträge** → **Eintrag hinzufügen**.
   b. Geben Sie das Suffix für Ihre Policy Director- und GSO-Benutzerdatenbank in das Feld **RDN des Eintrags** ein. Beispiel:

      `o=IBM,c=US`

   c. Klicken Sie auf **Organisation**.
   d. Klicken Sie auf **Weiter**.

      Das Fenster 'LDAP-Eintrag erstellen' wird angezeigt.

   e. Fügen Sie die entsprechenden Informationen für Ihre Organisation hinzu und klicken Sie dann auf die Schaltfläche **Erstellen**.
   f. Klicken Sie auf **Baumstruktur** → **Baumstruktur aktualisieren**. Der neue Eintrag sollte jetzt in der Verzeichnisstruktur zum Durchsuchen angezeigt werden.
5. Geben Sie der Policy Director-Sicherheitsdämongruppe die vollständige Steuerung, indem Sie folgende Angaben der Liste der Eigner jeder steuernden LDAP ACL hinzufügen:

   `cn=SecurityGroup,secAuthority=Default`

   Klicken Sie dazu auf die Registerkarte **ACL**.

   Das Fenster **Eine LDAP ACL bearbeiten** wird angezeigt.

   a. Geben Sie `cn=SecurityGroup,secAuthority=Default` in das Feld DN ein und klicken Sie dann auf **group** in der verdeckten Liste.
   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   c. Wählen Sie alle Kontrollkästchen unter Erteilte Berechtigungen für Hinzufügen, Löschen und Klasse aus.
   d. Klicken Sie anschließend auf **Ändern**. `cn=SecurityGroup,secAuthority=Default` sollte jetzt in der Liste der ACLs für Ihren Suffix-DN erscheinen.
   e. Wiederholen Sie die Prozedur für jedes Suffix, wenn mehrere Suffixe zur Liste der Eigner hinzugefügt werden sollen.

Die LDAP-Konfiguration ist jetzt abgeschlossen.

Installation von Policy Director für Windows

Die Abschnitte in diesem Kapitel beschreiben die Installation und Konfiguration von Policy Director auf den unterstützten Plattformen Windows und Windows NT.

Bevor Sie mit der Installation von Policy Director beginnen, stellen Sie sicher, daß Sie die Informationen in „Vor der Installation von Policy Director für Windows“ gelesen haben.

Vor der Installation von Policy Director für Windows

Bevor Sie mit der Installation von NetSEAT und Policy Director beginnen, lesen Sie die folgenden Informationen:

- Bevor Sie NetSEAT und Policy Director installieren, müssen Sie zuerst den Windows NT-Server installieren und konfigurieren.
- Sie müssen die Kennwörter für den Administrator der Windows NT-Domäne und für den Administrator der gesicherten Domäne (beispielsweise das cell_admin-Konto) kennen. Stellen Sie sicher, daß Sie über Administratorberechtigungen verfügen.
- Erstellen Sie bei der Installation der Policy Director-Server unter dem Betriebssystem Windows NT eine neue DCE-Zelle,
  - müssen Sie auch einen DCE-Server installieren und konfigurieren.
  - müssen Sie auch einen LDAP-Server installieren und konfigurieren, wenn Sie LDAP als Benutzerregistrierungsdatenbank verwenden.
- Machen Sie sich mit allen Informationen vertraut, die sich auf den Einsatz von Policy Director beziehen, wie in „Installationsvoraussetzungen für die gesicherte Domäne“ auf Seite 23 beschrieben.

NetSEAT und Policy Director installieren

Bevor Sie mit der Installation von Policy Director beginnen, schließen Sie alle Anwendungen. Nach der Installation von Policy Director müssen Sie einen Systemabschluß durchführen und den Computer erneut starten.

Informationen für die gesicherte Domäne vervollständigen

Während der Installation müssen Sie die folgenden für die Konfiguration Ihrer gesicherten Domäne spezifischen Informationen zur Verfügung stellen:

- Den Namen Ihrer gesicherten Domäne (DCE-Zelle), beispielsweise cell_admin.
- Die Namen der Computer, die die folgenden Services zur Verfügung stellen:
  - Sicherheit
  - Zeit
  - Cell Directory Services (CDS)
  - Directory Services Broker (DSB)

NetSEAT installieren

Die Policy Director NetSEAT-Konfigurationsdatei kopiert die NetSEAT-Dateien auf Ihre Festplatte und startet dann automatisch das NetSEAT-Konfigurationsdienstprogramm.

Gehen Sie wie folgt vor, um NetSEAT zu installieren:

1. Melden Sie sich als Benutzer mit Administratorberechtigungen an.
2. Legen Sie die CD *IBM SecureWay Policy Director Version 3.0* in das CD-ROM-Laufwerk ein.
3. Wechseln Sie in das Verzeichnis \win32\client auf der CD.
4. Klicken Sie doppelt auf die Datei Setup.exe. Das Programm InstallShield wird gestartet.
5. Wenn das Fenster 'Zu installierende Sprache auswählen' angezeigt wird, wählen Sie die entsprechende Sprache aus.
6. Klicken Sie auf **Weiter**. Das Willkommenfenster von Policy Director wird angezeigt.
7. Klicken Sie auf **Weiter**.
8. Wenn das Fenster 'Zu installierende Komponenten auswählen' angezeigt wird, klicken Sie auf **Client für Policy Director-Server-Produkte**.
9. Klicken Sie auf **Weiter**.
10. Wenn das Fenster 'Setup-Art auswählen' angezeigt wird, klicken Sie auf **Standard**.

    Die Standardposition für eine Standardinstallation lautet:

    ```
    c:\Programmdateien\ibm\netseat\
    ```

    Klicken Sie auf **Angepaßte Installation**, geben Sie das Laufwerk und das Verzeichnis an, in dem NetSEAT installiert werden soll. Das Fenster 'Zielpfad auswählen' wird angezeigt.
11. Klicken Sie auf **Weiter**.

    Die NetSEAT-Dateien werden in die NetSEAT-Standardposition auf Ihre Festplatte kopiert. Das NetSEAT-Konfigurationsfenster wird angezeigt.

NetSEAT konfigurieren

Mit den NetSEAT-Konfigurations-Tasks werden NetSEAT Informationen über die gesicherte Domäne zur Verfügung gestellt, wie beispielsweise DCE-Server-Namen, Standorte und Services.

Nachdem alle NetSEAT-Dateien auf das Festplattenlaufwerk kopiert wurden, wird das NetSEAT-Konfigurationsfenster (Registerkarte **Gesicherte Domänen**) angezeigt.

Gehen Sie wie folgt vor, um NetSEAT zu konfigurieren:

1. Soll ein Eintrag für eine neue gesicherte Domäne hinzugefügt werden, klicken Sie auf **Hinzufügen**.

   Das Fenster 'Neue gesicherte Domäne' wird angezeigt.

2. Geben Sie den Namen der gesicherten Domäne (DCE-Zelle) ein, zu der NetSEAT gehören soll, wie beispielsweise cell_admin.
3. Wählen Sie entweder das Kontrollkästchen **GSS aktivieren** oder das Kontrollkästchen **SSL aktivieren** aus.
4. Klicken Sie auf **OK**.

   Das Fenster 'Gesicherte Domäne - Eigenschaften' wird angezeigt.
5. Sollen ein DCE-Server und die Services, die von dem Server zur Verfügung gestellt werden, hinzugefügt werden, klicken Sie auf **Hinzufügen**.

   Das Fenster 'DCE-Server hinzufügen' wird angezeigt.

   Verwenden Sie dieses Fenster, um NetSEAT die vorhandenen DCE-Server in der gesicherten Domäne und die Services mitzuteilen, die von jedem Server zur Verfügung gestellt werden. Möglicherweise müssen Sie mehrere DCE-Server hinzufügen. Alle Services können sich auf einem Computer befinden oder können auf mehrere Computer verteilt werden.

   Mögliche Szenarios umfassen:

   - **Neue gesicherte Domäne (ein Host-System)**

     Wird eine neue gesicherte Domäne erstellt, die nur aus einem Host-System besteht, stellt das Host-System alle DCE-Services zur Verfügung. Geben Sie den Namen Ihres Host-Systems in das Feld **Maschinenname** ein. Wählen Sie einen oder mehrere Services aus. Wählen Sie den DSB aus, obwohl er noch nicht installiert ist.
   - **Neue gesicherte Domäne (mehrere Hosts)**

     Wird eine neue gesicherte Domäne erstellt und befinden sich die DCE-Services auf einem anderen Host, stellt Ihr lokaler Host nur den DSB-Service zur Verfügung. Fügen Sie in diesem Fall zuerst den DCE-Server hinzu, der die DCE-Services (Sicherheit, Zeit, CDS) zur Verfügung stellt. Fügen Sie dann einen anderen DCE-Server mit dem Namen `lokaler Host` zur Angabe Ihres lokalen Systems hinzu und wählen Sie das Kontrollkästchen DSB aus. Sie können den DSB auswählen, obwohl er noch nicht installiert ist.
   - **Vorhandene gesicherte Domäne**

     Wird Policy Director einer vorhandenen gesicherten Domäne hinzugefügt, fügen Sie den Namen des DCE-Servers hinzu, der die Services Sicherheit, Zeit und CDS zur Verfügung stellt. Geben Sie dann den Namen des DCE-Servers an, der den Policy Director-Verwaltungs-Server enthält, auf dem der DSB automatisch installiert wird. Wählen Sie das Kontrollkästchen DSB für dieses System aus. In diesem Szenario könnten sich alle Services, einschließlich DSB, auf demselben Host-System befinden.
6. Geben Sie für jeden Server den vollständigen DN-Maschinennamen eines vorhandenen Servers in der gesicherten Domäne ein (beispielsweise SFF98732.austin.ibm.com).

7. Wählen Sie für jeden Server einen oder mehrere der folgenden Services aus:
   - Sicherheit
   - DSB
   - Zeit
   - CDS
8. Klicken Sie auf **OK**.

   Der neue Eintrag wird im Fenster 'Gesicherte Domäne - Eigenschaften' angezeigt.
9. Wiederholen Sie bei Bedarf Schritt 5 auf Seite 47 bis Schritt 8, um weitere Server und Services hinzuzufügen.
10. Akzeptieren Sie im Fenster 'Gesicherte Domäne - Eigenschaften' die Standardkonfiguration für erweiterte Anmeldung **Nur DCE-Anmeldung**.

    Der Bereich für die integrierte Anmeldung im Fenster 'Gesicherte Domäne - Eigenschaften' wird in dieser NetSEAT-Installation nicht verwendet.
11. Klicken Sie auf **OK**.

    Das NetSEAT-Konfigurationsfenster wird angezeigt.
12. Klicken Sie auf **OK**.

    Das Fenster 'Systemwiederanlauf erforderlich' wird angezeigt.
13. Klicken Sie auf **Ja**, um den Computer erneut zu starten.
14. Klicken Sie auf **OK**.

    Beim Neustart des Computers wird NetSEAT automatisch gestartet. Ein NetSEAT-Symbol wird in der Windows-Task-Leiste angezeigt.

    Die Installation und Konfiguration von NetSEAT ist jetzt abgeschlossen.

NetSEAT-Client-Konfiguration prüfen

Prüfen Sie vor der Installation des Policy Director-Servers, ob der NetSEAT-Client in der angegebenen gesicherten Domäne erfolgreich konfiguriert wurde. Bestimmen Sie mit Hilfe von **netseat_ping**, ob die folgenden Services verfügbar sind:

- Sicherheitsservice
- Zeitservice
- Cell Directory Service
- Directory Services Broker (DSB)

Führen Sie die folgenden Schritte aus, um zu prüfen, ob der NetSEAT-Client mit den erforderlichen Services kommunizieren kann:

1. Klicken Sie auf **Start** → **Programme** → **NetSEAT** → **NetSEAT-Anmeldung**, um sich als cell_admin anzumelden.

   Sie können auch den Befehl **netseat_login** in eine Befehlszeile eingeben, um sich anzumelden.

2. Wählen Sie nicht die PKI-Anmeldung aus, wenn sie für Ihre Konfiguration nicht speziell erforderlich ist.

3. Geben Sie den Benutzernamen und das Kennwort des Policy Director-Administrators ein.

4. Klicken Sie auf **OK**.

5. Geben Sie den Befehl **netseat_ping** in die Befehlszeile ein, um den Konfigurationsstatus abzurufen.

   Ist beispielsweise ein NetSEAT-Client in der gesicherten Domäne "redback" konfiguriert, können Sie den Status durch Eingabe des folgenden Befehls in die DOS-Eingabeaufforderung abrufen:

   ```
   netseat_ping -C redback
   ```

   Es werden ähnliche Informationen wie in der folgenden Ausgabe angezeigt:

   ```
   /.../redback:
          Sicherheits-Server:
                       ncacn_ip_tcp:redback[ ] ist verfügbar
                       ncadg_ip_udp:redback[ ] ist verfügbar
          Cds-Server:
                       ncacn_ip_tcp:redback[ ] ist verfügbar
                       ncadg_ip_udp:redback[ ] ist verfügbar
          Zeit-Server:
                       ncacn_ip_tcp:redback[ ] ist verfügbar
                       ncadg_ip_udp:redback[ ] ist verfügbar
          Dsb-Server:
                       ncacn_ip_tcp:redback[ ] nicht verfügbar
                       ncacn_ip_udp:redback[ ] nicht verfügbar
   ```

   Beachten Sie jedoch, daß der DSB noch nicht ausgeführt wird, wenn eine neue gesicherte Domäne erstellt werden soll. In diesem Fall enthält die Ausgabe von **netseat_ping** für den DSB die Angabe `nicht verfügbar`. Diese Angabe ist die erwartete Ausgabe für dieses Szenario. Sie können mit der Installation von Policy Director unbesorgt fortfahren, da bei der Installation des Policy Director-Verwaltungs-Servers der DSB automatisch installiert, konfiguriert und gestartet wird. Wird der DSB bereits ausgeführt, zeigt die Ausgabe für den DSB die Angabe `ist verfügbar (v3.1)`.

6. Sind mit Ausnahme des DSB andere Services nicht verfügbar, beheben Sie den Fehler, bevor Sie die Policy Director-Server installieren.

Policy Director-Server installieren

Bevor Sie mit der Installation der Policy Director-Server beginnen, stellen Sie sicher, daß Sie den Benutzernamen und das Kennwort eines Administrators kennen.

Gehen Sie wie folgt vor, um die Policy Director-Server-Komponenten zu installieren:

1. Stellen Sie sicher, daß der LDAP-Server installiert und aktiv ist, wenn LDAP als Benutzerregistrierungsdatenbank verwendet werden soll. Vollständige Anweisungen befinden sich in „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29.
2. Legen Sie die CD *IBM SecureWay Policy Director Version 3.0* in das CD-ROM-Laufwerk ein.
3. Wechseln Sie in das Verzeichnis \win32\server auf der CD.
4. Klicken Sie auf die Datei Setup.exe. Das Programm InstallShield wird gestartet.
5. Wenn das Fenster 'Zu installierende Sprache auswählen' angezeigt wird, wählen Sie die entsprechende Sprache aus.
6. Klicken Sie auf **Weiter**. Das Willkommenfenster von Policy Director wird angezeigt.
7. Klicken Sie auf **Weiter**.

   Das Fenster 'Zielpfad auswählen' wird angezeigt.
8. Akzeptieren Sie die Standardverzeichnisposition für die Programmdateien oder klicken Sie auf die Schaltfläche **Durchsuchen**, um ein anderes Verzeichnis zu erstellen oder auszuwählen.

   Die Standardposition lautet: `C:\Programmdateien\IBM\`

   Wurde NetSEAT in einer Nicht-Standardposition installiert, installieren Sie die Policy Director-Server in derselben Position.
9. Klicken Sie auf **Weiter**.

   Das Fenster 'Komponenten auswählen' wird angezeigt.
10. Wählen Sie die entsprechenden Policy Director-Server-Komponenten aus. Der Abschnitt „Allgemeine Konfigurationen“ auf Seite 19 hilft Ihnen bei der Auswahl.

    In der gesicherten Domäne darf sich nur ein Exemplar des Policy Director-Verwaltungs-Servers (IVMgr) befinden.
11. Klicken Sie auf **Weiter**.
12. Haben Sie WebSEAL nicht ausgewählt, fahren Sie mit Schritt 14 auf Seite 51 fort.

    Haben Sie die WebSEAL-Komponente (IVWeb) ausgewählt, wird das Fenster 'Stammverzeichnis für Web-Dokument auswählen' angezeigt. In diesem Fenster werden Sie nach der Position des Stammverzeichnisses Ihres Web-Bereichs gefragt. Alle Ressourcen, die zu Ihrer Web-Site gehören, befinden sich unter diesem Verzeichnis.

13. Akzeptieren Sie die Standardposition des Stammverzeichnisses oder klicken Sie auf die Schaltfläche **Durchsuchen**, um ein anderes Verzeichnis zu erstellen oder auszuwählen. Die Standardposition lautet:

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

    Die Policy Director-Dateien werden jetzt von der CD auf das Festplattenlaufwerk kopiert. Das Anmeldefenster für den Administrator der gesicherten Domäne wird angezeigt. Dieser Schritt ist erforderlich, um die Sicherheitsberechtigung zu definieren und den Konfigurationsprozeß auszuführen.

14. Geben Sie den Namen und das Kennwort für den DCE-Zellenadministrator ein.

15. Haben Sie die Verwaltungs-Server-Komponente (IVMgr) ausgewählt, werden Sie aufgefordert, **LDAP-Registrierungsdatenbank** oder **DCE-Registrierungsdatenbank** auszuwählen.

    Haben Sie den Verwaltungs-Server nicht ausgewählt, wird die Art der Benutzerregistrierungsdatenbank für die vorhandene gesicherte Domäne automatisch erkannt:

    - Wird eine LDAP-Benutzerregistrierungsdatenbank erkannt, wird die Installation wie in „LDAP-Benutzerregistrierungsdatenbank verwenden“ auf Seite 52 beschrieben fortgesetzt.
    - Wird eine DCE-Benutzerregistrierungsdatenbank erkannt, wird die Installation wie in „DCE-Benutzerregistrierungsdatenbank verwenden“ auf Seite 53 beschrieben fortgesetzt.

16. Klicken Sie auf eine der folgenden Auswahlmöglichkeiten für die Benutzerregistrierungsdatenbank:

    - Wenn Sie auf **LDAP-Benutzerregistrierungsdatenbank** klicken, fahren Sie mit dem Abschnitt „LDAP-Benutzerregistrierungsdatenbank verwenden“ auf Seite 52 fort.
    - Wenn Sie auf **DCE-Benutzerregistrierungsdatenbank** klicken, fahren Sie mit dem Abschnitt „DCE-Benutzerregistrierungsdatenbank verwenden“ auf Seite 53 fort.

LDAP-Benutzerregistrierungsdatenbank verwenden

Verwendet Ihre gesicherte Policy Director-Domäne eine LDAP-Benutzerregistrierungsdatenbank, oder installieren Sie IVMgr und haben Sie **LDAP-Registrierungsdatenbank** ausgewählt, wird das Fenster 'LDAP-Server-Informationen' angezeigt.

1. Geben Sie die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:
   - LDAP-Host-Name
   - Port-Nummer
   - SSL-Port-Nummer (nur erforderlich, wenn SSL für den Zugriff auf den LDAP-Server verwendet wird)
   - LDAP-DN für GSO-Datenbank (beispielsweise o=ibm,c=us)
2. Klicken Sie auf **Weiter**.

   Das Fenster 'Kommunikation mit dem LDAP-Server' wird angezeigt.
3. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen Policy Director und dem LDAP-Server. Klicken Sie auf **Ja**, um die SSL-Übertragung zu aktivieren, oder klicken Sie auf **Nein**, um die SSL-Übertragung zu inaktivieren.

   Unter Windows NT wird die SSL-Übertragung einmal zwischen allen Policy Director-Servern auf dem Host-System und dem LDAP-Server aktiviert.

   Haben Sie die SSL-Übertragung aktiviert, fahren Sie mit Schritt 4 fort.

   Haben Sie die SSL-Übertragung inaktiviert, fahren Sie mit Schritt 5 fort.
4. Geben Sie für die folgenden Bedienerführungen Werte an:
   - Position der SSL-Schlüsseldatei
   - DN der SSL-Datei (Schlüsselkennsatz)
   - Kennwort für SSL-Schlüsseldatei

   Der Abschnitt „Datenbankschlüsseldatei und Zertifikat erstellen“ auf Seite 34 enthält weitere Informationen.
5. Klicken Sie auf **Weiter**.

   Das Fenster 'LDAP-Administratoranmeldung' wird angezeigt.
6. Geben Sie den Namen des LDAP-Administrators (beispielsweise cn=root) und das Kennwort ein und klicken Sie auf **OK**.

   Die Server werden konfiguriert und gestartet. Dies kann einige Minuten in Anspruch nehmen. Das Fenster 'Systeminformationen' wird mit dem Status der Server, einschließlich Registrierungsinformationen, angezeigt.
7. Klicken Sie auf **Weiter**.

   Das Fenster 'Policy Director-Setup beendet' wird angezeigt.

8. Klicken Sie auf **Ja**, um erneut zu starten. Haben Sie für den Neustart auf **Nein** geklickt, müssen Sie Windows NT zu einem späteren Zeitpunkt erneut starten, um den Konfigurationsprozeß abzuschließen. Damit ist die Policy Director-Installation abgeschlossen.
9. Klicken Sie auf **Beenden**.
   Sie werden aufgefordert, Ihr System erneut zu starten.

DCE-Benutzerregistrierungsdatenbank verwenden

Verwendet Ihre gesicherte Policy Director-Domäne eine DCE-Benutzerregistrierungsdatenbank, oder installieren Sie IVMgr und haben Sie **DCE-Benutzerregistrierungsdatenbank** ausgewählt, wird die Installation wie folgt fortgesetzt:

1. Haben Sie die WebSEAL-Komponente (IVWeb) ausgewählt, wird das Fenster 'Stammverzeichnis für Web-Dokument auswählen' angezeigt. In diesem Fenster wird die Position des Stammverzeichnisses Ihres Web-Bereichs angefordert. Alle Ressourcen, die zu Ihrer Web-Site gehören, befinden sich unter diesem Verzeichnis. Haben Sie WebSEAL nicht ausgewählt, fahren Sie mit Schritt 3 fort.
2. Akzeptieren Sie die Standardposition des Stammverzeichnisses oder klicken Sie auf die Schaltfläche **Durchsuchen**, um ein anderes Verzeichnis zu erstellen oder auszuwählen. Die Standardposition lautet:

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

3. Klicken Sie auf **Weiter**.

   Die Policy Director-Dateien werden jetzt von der CD auf das Festplattenlaufwerk kopiert. Das Anmeldefenster für den Administrator der gesicherten Domäne wird angezeigt.
4. Geben Sie den Namen des LDAP-Administrators und das Kennwort ein und klicken Sie dann auf **OK**. Die Server werden konfiguriert und gestartet. Dies kann einige Minuten in Anspruch nehmen. Das Fenster 'Systeminformationen' wird mit dem Status der Server, einschließlich Registrierungsinformationen, angezeigt.
5. Klicken Sie auf **Weiter**.

   Das Fenster 'Policy Director-Setup beendet' wird angezeigt.
6. Klicken Sie auf **Beenden**.

   Sie werden aufgefordert, Ihr System erneut zu starten.
7. Klicken Sie auf **Ja**, um erneut zu starten.

   Haben Sie für den Neustart auf **Nein** geklickt, müssen Sie Windows NT zu einem späteren Zeitpunkt erneut starten, um den Konfigurationsprozeß abzuschließen. Damit ist die Policy Director-Installation abgeschlossen.

Credentials Acquisition Service konfigurieren

Policy Director CAS wird automatisch installiert. Möchten Sie CAS als Ihren Credentials Acquisition Service verwenden, müssen Sie CAS konfigurieren. Die Informationen über die Konfiguration eines Credentials Acquisition Service im Handbuch *Policy Director Administration Guide* enthalten Anweisungen.

NetSEAL-Abfangroutine unter Windows NT verwenden

Policy Director NetSEAL (IVTrap) fängt Anforderungen für bestimmte Ports ab. Zur Verwendung der NetSEAL-Abfangroutine müssen Sie alle Anwendungen, die die angegebenen Ports verwenden, stoppen und erneut starten.

Weitere Informationen über die Konfiguration von Policy Director NetSEAL zum Abfangen von Anforderungen für bestimmte Ports enthält die Übersicht über NetSEAL im Handbuch *Policy Director Administration Guide*.

Verwaltungskonsole unter Windows installieren

Policy Director stellt eine Verwaltungskonsole zur Verfügung, mit der viele Komponenten des Policy Director-Sicherheitssystems von einem Windows-Client-Desktop verwaltet werden. Die Verwaltungskonsole kann unter den folgenden Betriebssystemen installiert werden:

- Windows 95
- Windows 98
- Windows NT Version 4.0 mit Service Pack 4 oder höher

Jedes Windows-Betriebssystem, unter dem Policy Director ausgeführt wird, erfordert den Policy Director NetSEAT-Client.

Der NetSEAT-Client kann entweder als DCE-Laufzeit-Client oder als Client für einen Policy Director-Server konfiguriert werden. Obwohl beide Konfigurationen von der Verwaltungskonsole akzeptiert werden, erfordern die Policy Director-Server den vollständigen Client für den Policy Director-Server.

Müssen Komponenten erneut installiert werden, muß die vorhandene Komponente entfernt werden, bevor sie erneut installiert wird.

Verwaltungskonsole mit Server-Komponenten installieren

Nachdem die Policy Director-Server-Komponenten im Abschnitt „Policy Director-Server installieren“ auf Seite 50 installiert und konfiguriert wurden, führen Sie die folgenden Schritte aus:

1. Legen Sie die CD *IBM SecureWay Policy Director Version 3.0* in das CD-ROM-Laufwerk ein.
2. Wechseln Sie in das Verzeichnis \win32\Console.
3. Klicken Sie doppelt auf die Datei Setup.exe. Das Programm InstallShield wird gestartet.
4. Wenn das Fenster 'Zu installierende Sprache auswählen' angezeigt wird, wählen Sie die entsprechende Sprache aus.
5. Klicken Sie auf **Weiter**. Das Willkommenfenster von Policy Director wird angezeigt.
6. Klicken Sie auf **Weiter**. Das Fenster 'Zielpfad auswählen' wird angezeigt.
7. Geben Sie eine Position an, an der die Dateien installiert werden sollen.

   Die Dateien werden in ihre korrekten Positionen auf dem Windows-Computer kopiert. Ein Informationsfenster wird angezeigt, in dem eine erfolgreiche Installation angegeben wird.
8. Werden Sie gefragt, ob Windows erneut gestartet werden soll, klicken Sie auf **Ja**.
9. Klicken Sie auf **OK**.
10. Fahren Sie mit „Verwaltungskonsole starten“ auf Seite 56 fort.

Verwaltungskonsole ohne Server-Komponenten installieren

Um die Verwaltung der Policy Director-Sicherheit von zusätzlichen Windows-Systemen zu ermöglichen, können Sie die Verwaltungskonsole auf Windows-Systemen installieren, für die die Policy Director-Server-Komponenten nicht installiert sind. Wird die Verwaltungskonsole auf diese Art und Weise installiert, kann der NetSEAT-Client entweder als DCE-Laufzeit-Client oder als Client für einen Policy Director-Server konfiguriert werden.

Soll die Verwaltungskonsole ohne die Server-Komponenten installiert werden, verwenden Sie das Windows-Desktop-System und führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, daß das Windows-Betriebssystem eine unterstützte Plattform ist. Siehe „Policy Director-Server“ auf Seite 16.
2. Installieren Sie den Policy Director NetSEAT-Client. Befolgen Sie die Anweisungen in „NetSEAT installieren“ auf Seite 46.
3. Stellen Sie sicher, daß der NetSEAT-Client ordnungsgemäß in der gesicherten Domäne konfiguriert ist, in der die Verwaltungskonsole ausgeführt wird. Siehe „NetSEAT-Client-Konfiguration prüfen“ auf Seite 48.
4. Legen Sie die CD *IBM SecureWay Policy Director Version 3.0* in das CD-ROM-Laufwerk ein.
5. Wechseln Sie in das Verzeichnis \win32\Console.
6. Klicken Sie doppelt auf die Datei Setup.exe. Das Programm InstallShield wird gestartet.
7. Wenn das Fenster 'Zu installierende Sprache auswählen' angezeigt wird, wählen Sie die entsprechende Sprache aus.
8. Klicken Sie auf **Weiter**. Das Willkommenfenster von Policy Director wird angezeigt.
9. Klicken Sie auf **Weiter**. Das Fenster 'Zielpfad auswählen' wird angezeigt.
10. Geben Sie eine Position an, an der die Dateien installiert werden sollen.

    Die Dateien werden in ihre korrekten Positionen auf dem Windows-Computer kopiert. Ein Informationsfenster wird angezeigt, in dem eine erfolgreiche Installation angegeben wird.
11. Klicken Sie auf **OK**, um die Installation abzuschließen.
12. Fahren Sie mit „Verwaltungskonsole starten“ fort, um die Verwaltungskonsole zu starten.

Verwaltungskonsole starten

Gehen Sie wie folgt vor, um die Verwaltungskonsole zu starten:

1. Stellen Sie sicher, daß die Policy Director-Server installiert und aktiv sind.
2. Klicken Sie auf **Start → Programme → Policy Director → Verwaltungskonsole.**

   Das Fenster 'Policy Director-Verwaltungskonsole' wird angezeigt.
3. Melden Sie sich bei der Verwaltungskonsole als Benutzer mit Administratorberechtigungen an, beispielsweise als cell_admin.

Policy Director entfernen

Um Policy Director-Komponenten zu entfernen, müssen Sie sich als Administrator anmelden. Melden Sie sich bei der Windows-Domäne als Benutzer mit Administratorberechtigung an. Beispiel:

```
dce_login cell_admin Kennwort
```

Wird versucht, eine Komponente ohne die korrekte Berechtigung für die gesicherte Domäne zu entfernen, wird ein Nachrichtenfenster mit einem Berechtigungsfehler angezeigt.

Sie müssen Policy Director-Komponenten in exakt umgekehrter Installationsreihenfolge entfernen. Verwenden Sie das Symbol **Programme hinzufügen/entfernen** in der Systemsteuerung, um Policy Director zu entfernen.

Soll eine vollständige Policy Director-Installation deinstalliert werden, führen Sie die folgenden Prozeduren in der angegebenen Reihenfolge aus:

1. Verwaltungskonsole entfernen.
2. Server-Komponenten entfernen.
3. NetSEAT-Client entfernen.

Verwaltungskonsole entfernen

Gehen Sie wie folgt vor, um die Verwaltungskonsole zu entfernen:

1. Ist die Verwaltungskonsole aktiv, muß sie geschlossen werden.
2. Verwenden Sie **Programme hinzufügen/entfernen** in der Systemsteuerung und klicken Sie auf **Policy Director-Verwaltungskonsole.**
3. Klicken Sie auf die Schaltfläche **Hinzufügen/Entfernen**.
4. Sie werden aufgefordert, das Entfernen des Programms zu bestätigen. Klicken Sie dazu auf **Ja**.
5. Klicken Sie auf **OK**.

Server-Komponenten entfernen

Zum Entfernen der Policy Director-Server-Komponenten müssen Sie über die entsprechenden Berechtigungen verfügen. Erst dann können Sie die Komponenten entfernen.

Gehen Sie wie folgt vor, um Server-Komponenten zu entfernen:

1. Stellen Sie sicher, daß die Policy Director-Server installiert und aktiv sind.
2. Verwenden Sie **Programme hinzufügen/entfernen** in der Systemsteuerung und wählen Sie dann die erste Policy Director-Server-Komponente aus, die entfernt werden soll.
3. Entfernen Sie die Policy Director-Server-Komponenten in exakt umgekehrter Installationsreihenfolge.

   Haben Sie beispielsweise alle Komponenten installiert, entfernen Sie die Komponenten in der folgenden Reihenfolge:

   - Authorization ADK (IVAuthADK)
   - Berechtigungs-Server (IVAcld)
   - NetSEAL (IVTrap)
   - WebSEAL (IVWeb)
   - Sicherheitsmanager (IVNet)
   - Verwaltungs-Server (IVMgr)
   - Basis (IVBase). Diese Komponente wird immer automatisch installiert.

   Die Policy Director-Verwaltungskonsole kann jederzeit entfernt werden. Weitere Informationen über die Reihenfolge, in der Komponenten installiert werden, befinden sich im Abschnitt „Übersicht über die schrittweise Installation von Policy Director“ auf Seite 25.
4. Klicken Sie auf die Schaltfläche **Hinzufügen/Entfernen**.
5. Geben Sie den Benutzernamen und das Kennwort des LDAP-Administrators ein, wenn Sie dazu aufgefordert werden.
6. Wiederholen Sie Schritt 2 bis Schritt 5 für jede Policy Director-Server-Komponente.
7. Klicken Sie abschließend auf **OK**.

NetSEAT-Client entfernen

Sie müssen über Windows NT-Administratorberechtigungen verfügen, um Policy Director NetSEAT-Komponenten entfernen zu können.

1. Verwenden Sie **Programme hinzufügen/entfernen** in der Systemsteuerung und klicken Sie dann auf die Registerkarte **Installieren/Deinstallieren**.
2. Klicken Sie im Listenfenster der Registerkarte auf **Policy Director NetSEAT-Client**.
3. Klicken Sie auf **Hinzufügen/Entfernen**.
4. Klicken Sie auf **OK**.

Installation von Policy Director für AIX

Die Abschnitte in diesem Kapitel beschreiben die Installation und Konfiguration von Policy Director unter dem Betriebssystem AIX.

Bevor Sie mit der Installation von Policy Director beginnen, stellen Sie sicher, daß Sie die Informationen in „Vor der Installation von Policy Director für AIX“ gelesen haben.

Vor der Installation von Policy Director für AIX

Bevor Sie mit der Installation von NetSEAT und Policy Director beginnen, lesen Sie die folgenden Informationen:

- Erstellen Sie bei der Installation der Policy Director-Server eine neue DCE-Zelle,
  - müssen Sie auch einen DCE-Server installieren und konfigurieren.
  - müssen Sie auch einen LDAP-Server installieren und konfigurieren, wenn Sie LDAP als Benutzerregistrierungsdatenbank verwenden.
- Machen Sie sich mit allen Informationen vertraut, die sich auf den Einsatz von Policy Director beziehen, wie in „Installationsvoraussetzungen für die gesicherte Domäne“ auf Seite 23 beschrieben.

Verwaltungskonsole installieren

Policy Director stellt eine Verwaltungskonsole zur Verfügung, mit der alle Komponenten des Policy Director-Systems verwaltet werden können. Administratoren können auswählen, ob die Verwaltungskonsole auf einem AIX-System und/oder einem Windows-System installiert werden soll. Die Verwaltungskonsole für AIX wird als Paket mit dem Namen IV.Console verteilt. Verwenden Sie SMIT, um das Paket zu installieren und zu konfigurieren.

Policy Director installieren

Verwenden Sie die folgenden Anweisungen, um Policy Director für AIX zu installieren:

1. Stellen Sie sicher, daß der LDAP-Server installiert und aktiv ist, wenn LDAP als Benutzerregistrierungsdatenbank verwendet werden soll. Vollständige Anweisungen befinden sich in „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29.
2. Melden Sie sich als Root an.
3. Legen Sie die CD *IBM SecureWay Policy Director Version 3.0* in das CD-ROM-Laufwerk ein.
4. Starten Sie SMIT.
5. Klicken Sie auf **Softwareinstallation und Wartung**.

   Das Menü 'Softwareinstallation und Wartung' wird angezeigt.

6. Klicken Sie auf **Software installieren und aktualisieren**.

   Das Menü 'Software installieren und aktualisieren' wird angezeigt.

7. Klicken Sie auf **Software durch Paketname installieren/aktualisieren**.
   Das Fenster 'Software durch Paketname installieren/aktualisieren' wird angezeigt.

8. Geben Sie den Namen der Einheit ein, von der die Software installiert werden soll.

   Beispiel:

   - Erfolgt die Installation über eine CD-Einheit, könnten Sie folgendes eingeben: `/dev/cd0`
   - Erfolgt die Installation aus einem Verzeichnis auf einem angehängten Server, könnten Sie folgendes eingeben: `/mnt/user/lpp/IV`

     Nach der Eingabe des Einheitennamens wird das Fenster 'Liste - Mehrfachauswahl' angezeigt.

9. Klicken Sie auf **IV**.
   Im Fenster 'Liste - Mehrfachauswahl' wird die Liste der Policy Director-Softwarepakete angezeigt.

10. Wählen Sie die Pakete aus, die installiert werden sollen.

    - Sollen alle Policy Director-Pakete installiert werden, klicken Sie auf den Eintrag **IV**.
    - Sollen nur einige der Policy Director-Pakete installiert werden, beachten Sie die Installationsabhängigkeiten, die im Abschnitt „Installationsvoraussetzungen für die gesicherte Domäne“ auf Seite 23 beschrieben sind.

11. Klicken Sie auf **OK**.

    Das SMIT-Menü 'Software durch Paketname installieren/aktualisieren' wird angezeigt.

12. Klicken Sie auf **Ja** für das Feld, das wie folgt bezeichnet ist:

    `Vorausgesetzte Software AUTOMATISCH installieren?`

    Mit diesem Schritt wird sichergestellt, daß die Pakete Policy Director-Basis (IV.Base) und SMIT-Setup (IV.smit) installiert werden. Diese Pakete sind vorausgesetzte Software für die anderen Policy Director-Pakete. Wird dieses Feld auf **Nein** gesetzt, kehren Sie zum Paketauswahlmenü zurück. Stellen Sie sicher, daß Sie IV.Base und IV.Smit ausgewählt haben.

13. Setzen Sie die anderen Felder auf Werte, die für Ihre Installation geeignet sind.

14. Klicken Sie auf **OK**.

    SMIT zeigt Statusnachrichten an, einschließlich:

    - Vorinstallationsprüfung der Policy Director-Softwarepakete.
    - Name jedes Pakets während der Extraktion der Dateien aus dem Paket.
    - Erstellung von Konfigurationsmenüs für jedes Paket.
    - Statusnachricht, die die erfolgreiche Beendigung des Dateiauszugs angibt.

15. Ist der Dateiauszug beendet, konfigurieren Sie die Policy Director-Pakete unter Verwendung der Informationen in "Policy Director mit einer LDAP-Benutzerregistrierungsdatenbank konfigurieren". Wird die DCE-Registrierungsdatenbank verwendet, lesen Sie die Informationen in „Policy Director mit einer DCE-Benutzerregistrierungsdatenbank konfigurieren“ auf Seite 68.

Policy Director mit einer LDAP-Benutzerregistrierungsdatenbank konfigurieren

Sie müssen die Policy Director-Softwarepakete installieren, bevor Sie die Pakete konfigurieren können. Wurden die Policy Director-Pakete noch nicht installiert, lesen Sie die Informationen in „Policy Director installieren“ auf Seite 59.

Haben Sie Policy Director mit einer DCE-Benutzerregistrierungsdatenbank installiert, fahren Sie mit dem Abschnitt „Policy Director mit einer DCE-Benutzerregistrierungsdatenbank konfigurieren“ auf Seite 68 fort.

Sie müssen jedes installierte Policy Director-Paket konfigurieren, mit Ausnahme von SMIT-Setup. Konfigurieren Sie jeweils ein Paket. Bei einigen Policy Director-Paketen ist es erforderlich, daß der Administrator während der Konfiguration auf Eingabeaufforderungen antwortet.

Gehen Sie wie folgt vor, um die Policy Director-Pakete zu konfigurieren:

1. Starten Sie SMIT.

   Das Menü 'Systemverwaltung' wird angezeigt.

2. Klicken Sie auf **Netzkommunikation und -anwendungen**.

   Eine Liste der installierten Softwarepakete wird angezeigt. Beispiel:

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

3. Klicken Sie auf **Policy Director**.

   Das Policy Director-Menü wird mit den folgenden Optionen angezeigt:

   - Policy Director - Konfiguration
   - Policy Director - Dekonfiguration

4. Klicken Sie auf **Policy Director - Konfiguration**.

   Eine Liste der installierten Policy Director-Pakete wird angezeigt, wie beispielsweise:

   - Policy Director-Basis - Konfiguration
   - Policy Director-Verwaltungs-Server - Konfiguration
   - Policy Director-Verwaltungskonsole - Konfiguration

- Policy Director-Sicherheitsmanager - Konfiguration
- Policy Director WebSEAL - Konfiguration
- Policy Director-Berechtigungs-Server - Konfiguration
- Policy Director NetSEAL - Konfiguration
- Policy Director Authorization ADK - Konfiguration

5. Klicken Sie jeweils auf ein Paket, das konfiguriert werden soll.

   Sie müssen die Policy Director-Pakete in der Reihenfolge konfigurieren, in der sie in der Policy Director-Konfigurationsliste erscheinen. Wählen Sie jeweils ein Paket aus, und zwar vom ersten Eintrag in der Liste bis zum letzten Eintrag in der Liste.

Sie müssen jetzt die ausgewählten Policy Director-Pakete unter Verwendung der entsprechenden Konfigurationsanweisungen in den folgenden Abschnitten konfigurieren.

Basispaket konfigurieren

Das Basispaket wird auf einem Computer installiert, wenn eines der anderen Pakete installiert wird. Zum Konfigurieren des Basispakets klicken Sie auf **Policy Director-Basis** in der Policy Director-Konfigurationsliste.

Die Konfiguration des Policy Director-Basispakets erfolgt ohne Eingaben des Benutzers.

Verwaltungs-Server konfigurieren

Gehen Sie wie folgt vor, um den Verwaltungs-Server zu konfigurieren:

1. Klicken Sie auf **Policy Director-Verwaltungs-Server** in der Policy Director-Konfigurationsliste.

   Es erscheint eine Eingabeaufforderung, in der Sie aufgefordert werden, eine Art der Benutzerregistrierungsdatenbank auszuwählen.

2. Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, geben Sie eine 2 für LDAP-Benutzerregistrierungsdatenbank ein.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

3. Geben Sie auf Anforderung den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, wird eine Reihe von Eingabeaufforderungen zum Konfigurieren der Kommunikation zwischen dem Verwaltungs-Server und dem LDAP-Server angezeigt.

4. Geben Sie die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:

   - Host-Name des LDAP-Servers
   - Port-Nummer des LDAP-Servers
   - SSL-Port-Nummer des LDAP-Servers (wahlfrei)

5. Geben Sie den Benutzernamen und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein (beispielsweise `cn=root`). Die Policy Director-Sicherheitsinformationen werden jetzt mit dem LDAP-Server registriert.
6. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen dem Verwaltungs-Server und dem LDAP-Server.

   Anmerkung: Sie können die SSL-Übertragung zwischen jedem Server und dem LDAP-Server individuell aktivieren oder inaktivieren. In diesem Fall wird die SSL-Übertragung zwischen dem Verwaltungs-Server (IVMgr) und dem LDAP-Server konfiguriert.
7. Wurde die SSL-Übertragung inaktiviert, fahren Sie mit Schritt 8 fort. Haben Sie die SSL-Übertragung aktiviert, geben Sie Werte für die folgenden Eingabeaufforderungen an:
   - Position der SSL-Schlüsseldatei
   - SSL-Schlüsselkennsatz
   - Kennwort für SSL-Schlüsseldatei
8. Aktivieren Sie den GSO-Datenbankzugriff, indem Sie den DN für das GSO-Datenbanksuffix zur Verfügung stellen, das Sie in „Suffixe hinzufügen“ auf Seite 30 hinzugefügt haben.

   Beispiel:

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

   Nachdem der GSO-Datenbankzugriff konfiguriert wurde, konfiguriert der Policy Director-Konfigurationsmanager automatisch einen Directory Services Broker. In einer Reihe von Nachrichten wird jeder automatisierte Schritt bei seiner Beendigung aufgelistet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVMgr-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Verwaltungskonsole konfigurieren und starten

Zum Konfigurieren der Verwaltungskonsole klicken Sie auf **Policy Director-Verwaltungskonsole** in der Policy Director-Konfigurationsliste.

Die Konfiguration der Policy Director-Verwaltungskonsole erfolgt ohne Eingaben des Benutzers.

Gehen Sie wie folgt vor, um die AIX-Version der Verwaltungskonsole zu starten:

1. Stellen Sie sicher, daß die Policy Director-Server installiert und aktiv sind.
2. Geben Sie den folgenden Befehl ein:

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

Verwenden Sie die Windows-Client-Version der Verwaltungskonsole, befolgen Sie die Anweisungen in „Verwaltungskonsole starten“ auf Seite 56.

Sicherheitsmanager konfigurieren

Gehen Sie wie folgt vor, um den Sicherheitsmanager (IVNet) zu konfigurieren:

1. Klicken Sie auf **Policy Director-Sicherheitsmanager** in der Policy Director-Konfigurationsliste.

   Eine Reihe von Eingabeaufforderungen wird angezeigt, um den Sicherheitsmanager mit dem LDAP-Server zu integrieren.

2. Geben Sie auf Anforderung die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:

   - Host-Name des LDAP-Servers
   - Port-Nummer des LDAP-Servers
   - SSL-Port-Nummer des LDAP-Servers (wahlfrei)

   Diese Eingabeaufforderungen werden nicht angezeigt, wenn zuvor der Policy Director-Verwaltungs-Server oder der Berechtigungs-Server konfiguriert wurde.

3. Geben Sie den Benutzernamen und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein. Die Policy Director-Sicherheitsinformationen werden jetzt mit dem LDAP-Server registriert.

4. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen dem Sicherheitsmanager und dem LDAP-Server.

   Anmerkung: Sie können die SSL-Übertragung zwischen jedem Policy Director-Server und dem LDAP-Server individuell aktivieren oder inaktivieren. In diesem Fall wird die SSL-Übertragung zwischen dem Sicherheitsmanager (IVNet, zur Verwendung durch WebSEAL und NetSEAL) und dem LDAP-Server konfiguriert.

5. Wurde die SSL-Übertragung inaktiviert, fahren Sie mit Schritt 6 fort. Haben Sie die SSL-Übertragung aktiviert, geben Sie Werte für die folgenden Eingabeaufforderungen an:

   - Position der SSL-Schlüsseldatei
   - SSL-Schlüsselkennsatz
   - Kennwort für SSL-Schlüsseldatei

6. Aktivieren Sie den GSO-Datenbankzugriff, indem Sie den DN für das GSO-Datenbanksuffix zur Verfügung stellen, das Sie in „Suffixe hinzufügen“ auf Seite 30 hinzugefügt haben.

   Beispiel:

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

   Diese Eingabeaufforderung wird nicht angezeigt, wenn zuvor der Policy Director-Verwaltungs-Server oder der Berechtigungs-Server konfiguriert wurde.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

7. Geben Sie auf Anforderung den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Der Sicherheitsmanager wird konfiguriert und gestartet. Der CAS-Server wird ebenfalls gestartet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des Sicherheitsmanagers angegeben ist.

Policy Director WebSEAL konfigurieren

Gehen Sie wie folgt vor, um Policy Director WebSEAL (IVWeb) zu konfigurieren:

1. Klicken Sie auf **Policy Director WebSEAL** in der Policy Director-Konfigurationsliste.

   Das Policy Director WebSEAL-Konfigurationsmenü wird mit Werten angezeigt, die folgendes bestätigen:

   - HTTP- und HTTPS-Client-Zugriff
   - Erforderliche TCP-Ports (TCP = Transmission Control Protocol)
   - Standardstammverzeichnis für Web-Dokument

2. Bestätigen Sie die aktuellen Konfigurationswerte:

```
Web-Server-Konfiguration überprüfen:
1. TCP HTTP aktivieren?              Ja
2. HTTP-Port                         80
3. HTTPS aktivieren?                 Ja
4. HTTPS-Port                        443
5. Web-Dokumentstammverzeichnis      /opt/Policy Director/www/docs
a. Konfiguration akzeptieren und Installation fortsetzen
x. Installation verlassen

Zu ändernden Eintrag auswählen: a
```

3. Geben Sie `a` ein, um die Konfiguration zu akzeptieren und die Installation fortzusetzen, oder geben Sie die Nummer für den Wert ein, der geändert werden soll.

   Die Konfiguration des Policy Director-Sicherheitsmanagers fordert Sie auf, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

4. Geben Sie den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Der Policy Director-Sicherheitsmanager wird erneut gestartet.

   Die Installation konfiguriert und aktiviert Policy Director WebSEAL auf dem Computer.

Policy Director-Berechtigungs-Server konfigurieren

Gehen Sie wie folgt vor, um den Policy Director-Berechtigungs-Server (IVAcld) zu konfigurieren:

1. Klicken Sie auf **Policy Director-Berechtigungs-Server** in der Policy Director-Konfigurationsliste.

   Es erscheinen eine oder mehrere Eingabeaufforderungen, um den Policy Director-Berechtigungs-Server mit dem LDAP-Server zu integrieren.

2. Geben Sie auf Anforderung die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:

   - Host-Name des LDAP-Servers
   - Port-Nummer des LDAP-Servers
   - SSL-Port-Nummer des LDAP-Servers (wahlfrei)

   Diese Eingabeaufforderungen werden nicht angezeigt, wenn zuvor der Policy Director-Verwaltungs-Server oder der Berechtigungs-Server konfiguriert wurde.

3. Geben Sie den Benutzernamen und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein. Die Policy Director-Sicherheitsinformationen werden jetzt mit dem LDAP-Server registriert.

4. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen dem Sicherheitsmanager und dem LDAP-Server.

   Anmerkung: Sie können die SSL-Übertragung zwischen jedem Policy Director-Server und dem LDAP-Server individuell aktivieren oder inaktivieren. In diesem Fall wird die SSL-Übertragung zwischen dem Berechtigungs-Server (IVAcld) und dem LDAP-Server konfiguriert.

5. Wurde die SSL-Übertragung inaktiviert, fahren Sie mit Schritt 6 fort. Haben Sie die SSL-Übertragung aktiviert, geben Sie Werte für die folgenden Eingabeaufforderungen an:

   - Position der SSL-Schlüsseldatei
   - SSL-Schlüsselkennsatz
   - Kennwort für SSL-Schlüsseldatei

6. Aktivieren Sie den GSO-Datenbankzugriff, indem Sie den DN für das GSO-Datenbanksuffix zur Verfügung stellen, das Sie in „Suffixe hinzufügen“ auf Seite 30 hinzugefügt haben.

   Beispiel:

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

   Diese Eingabeaufforderung wird nicht angezeigt, wenn zuvor der Policy Director-Verwaltungs-Server oder der Berechtigungs-Server konfiguriert wurde.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

7. Geben Sie auf Anforderung den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Der Berechtigungs-Server wird konfiguriert und gestartet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des Berechtigungs-Servers angegeben ist.

Policy Director NetSEAL konfigurieren

Gehen Sie wie folgt vor, um Policy Director NetSEAL zu konfigurieren:

1. Klicken Sie auf **Policy Director NetSEAL** in der Policy Director-Konfigurationsliste.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie den Benutzernamen und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein. Die Policy Director-Sicherheitsinformationen werden jetzt mit dem LDAP-Server registriert.

   Die Konfiguration des Policy Director NetSEAL-Pakets wird ausgeführt.

Policy Director NetSEAL fängt Anforderungen an bestimmte Ports ab. Zur Verwendung der NetSEAL-Abfangroutine müssen Sie alle Anwendungen, die die angegebenen Ports verwenden, stoppen und erneut starten. Weitere Informationen über die Verwendung von Policy Director NetSEAL befinden sich im Abschnitt „NetSEAL-Abfangroutine unter AIX verwenden“ auf Seite 72.

Policy Director Authorization ADK konfigurieren

Zum Konfigurieren des Policy Director Authorization ADK klicken Sie auf **Policy Director Authorization ADK** in der Policy Director-Konfigurationsliste.

Die Konfiguration des Policy Director Authorization ADK erfolgt ohne Eingaben des Benutzers.

Policy Director Credentials Acquisition Service konfigurieren

Policy Director CAS wird automatisch installiert. Möchten Sie Policy Director CAS als Ihren Credentials Acquisition Service verwenden, müssen Sie CAS konfigurieren. Informationen über Policy Director CAS und über die Konfiguration von CAS für den WebSEAL-Server befinden sich in dem Handbuch *Policy Director Administration Guide*.

Policy Director mit einer DCE-Benutzerregistrierungsdatenbank konfigurieren

Sie müssen die Policy Director-Softwarepakete installieren, bevor Sie die Pakete konfigurieren können. Wurden die Policy Director-Pakete noch nicht installiert, lesen Sie zuerst die Informationen in „Policy Director installieren“ auf Seite 59.

Haben Sie Policy Director mit einer LDAP-Benutzerregistrierungsdatenbank installiert, fahren Sie mit dem Abschnitt „Policy Director mit einer LDAP-Benutzerregistrierungsdatenbank konfigurieren“ auf Seite 61 fort.

Sie müssen jedes installierte Policy Director-Paket konfigurieren, mit Ausnahme von SMIT-Setup. Konfigurieren Sie jeweils ein Paket. Bei einigen Policy Director-Paketen ist es erforderlich, daß der Administrator während der Konfiguration auf Eingabeaufforderungen antwortet.

Gehen Sie wie folgt vor, um die Policy Director-Pakete zu konfigurieren:

1. Starten Sie SMIT.

   Das Menü 'Systemverwaltung' wird angezeigt.

2. Klicken Sie auf **Netzkommunikation und -anwendungen**.

   Eine Liste der installierten Softwarepakete wird angezeigt. Beispiel:

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

3. Klicken Sie auf **Policy Director**.

   Das Policy Director-Menü wird mit den folgenden Optionen angezeigt:

   - Policy Director - Konfiguration
   - Policy Director - Dekonfiguration

4. Klicken Sie auf **Policy Director - Konfiguration**.

   Eine Liste der installierten Policy Director-Pakete wird angezeigt, wie beispielsweise:

   - Policy Director-Basis - Konfiguration
   - Policy Director-Verwaltungs-Server - Konfiguration
   - Policy Director-Verwaltungskonsole - Konfiguration
   - Policy Director-Sicherheitsmanager - Konfiguration
   - Policy Director WebSEAL - Konfiguration
   - Policy Director-Berechtigungs-Server - Konfiguration
   - Policy Director NetSEAL - Konfiguration
   - Policy Director Authorization ADK - Konfiguration

5. Klicken Sie jeweils auf ein Paket, das konfiguriert werden soll.

   Sie müssen die Policy Director-Pakete in der Reihenfolge konfigurieren, in der sie in der Policy Director-Konfigurationsliste erscheinen. Wählen Sie jeweils ein Paket aus, und zwar vom ersten Eintrag in der Liste bis zum letzten Eintrag in der Liste.

Sie müssen jetzt die ausgewählten Policy Director-Pakete unter Verwendung der entsprechenden Konfigurationsanweisungen in den folgenden Abschnitten konfigurieren.

Basispaket konfigurieren

Das Basispaket wird auf einem Computer installiert, wenn eines der anderen Pakete installiert wird. Zum Konfigurieren des Basispakets klicken Sie auf **Policy Director-Basis** in der Policy Director-Konfigurationsliste.

Die Konfiguration des Policy Director-Basispakets erfolgt ohne Eingaben des Benutzers.

Verwaltungs-Server konfigurieren

Gehen Sie wie folgt vor, um den Verwaltungs-Server zu konfigurieren:

1. Klicken Sie auf **Policy Director-Verwaltungs-Server** in der Policy Director-Konfigurationsliste.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie auf Anforderung den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Die Installation konfiguriert und startet den Verwaltungs-Server.

Verwaltungskonsole konfigurieren und starten

Zum Konfigurieren der Verwaltungskonsole klicken Sie auf **Policy Director-Verwaltungskonsole** in der Policy Director-Konfigurationsliste.

Die Konfiguration der Policy Director-Verwaltungskonsole erfolgt ohne Eingaben des Benutzers.

Gehen Sie wie folgt vor, um die AIX-Version der Verwaltungskonsole zu starten:

1. Stellen Sie sicher, daß die Policy Director-Server installiert und aktiv sind.
2. Geben Sie den folgenden Befehl ein:

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

Sicherheitsmanager konfigurieren

Gehen Sie wie folgt vor, um den Sicherheitsmanager (IVNet) zu konfigurieren:

1. Klicken Sie auf **Policy Director-Sicherheitsmanager** in der Policy Director-Konfigurationsliste.
2. Geben Sie auf Anforderung den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

Die Installation konfiguriert und startet den Sicherheitsmanager.

Policy Director WebSEAL konfigurieren

Gehen Sie wie folgt vor, um Policy Director WebSEAL (IVWeb) zu konfigurieren:

1. Klicken Sie auf **Policy Director WebSEAL** in der Policy Director-Konfigurationsliste.

   Das Policy Director WebSEAL-Konfigurationsmenü wird mit Werten angezeigt, die folgendes bestätigen:

   - HTTP- und HTTPS-Client-Zugriff
   - Erforderliche TCP-Ports (TCP = Transmission Control Protocol)
   - Standardstammverzeichnis für Web-Dokument

2. Bestätigen Sie die aktuellen Konfigurationswerte:

```
Web-Server-Konfiguration überprüfen:
1. TCP HTTP aktivieren?              Ja
2. HTTP-Port                         80
3. HTTPS aktivieren?                 Ja
4. HTTPS-Port                        443
5. Web-Dokumentstammverzeichnis      /opt/Policy Director/www/docs
a. Konfiguration akzeptieren und Installation fortsetzen
x. Installation verlassen

Zu ändernden Eintrag auswählen: a
```

3. Geben Sie `a` ein, um die Konfiguration zu akzeptieren und die Installation fortzusetzen, oder geben Sie die Nummer für den Wert ein, der geändert werden soll.

   Die Konfiguration des Policy Director-Sicherheitsmanagers fordert Sie auf, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

4. Geben Sie den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Der Policy Director-Sicherheitsmanager wird erneut gestartet.

   Die Installation konfiguriert und aktiviert Policy Director WebSEAL auf dem Computer.

Policy Director-Berechtigungs-Server konfigurieren

Gehen Sie wie folgt vor, um den Policy Director-Berechtigungs-Server (IVAcld) zu konfigurieren:

1. Klicken Sie auf **Policy Director-Berechtigungs-Server** in der Policy Director-Konfigurationsliste.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie den Kontonamen und das Kennwort des DCE-Zellenadministrators ein.

   Der Berechtigungs-Server wird konfiguriert und gestartet.

Policy Director NetSEAL konfigurieren

Gehen Sie wie folgt vor, um Policy Director NetSEAL zu konfigurieren:

1. Klicken Sie auf **Policy Director NetSEAL** in der Policy Director-Konfigurationsliste.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie den Benutzernamen und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein. Die Policy Director-Sicherheitsinformationen werden jetzt mit dem LDAP-Server registriert.

   Die Policy Director NetSEAL-Konfiguration wird ausgeführt.

Policy Director NetSEAL fängt Anforderungen an bestimmte Ports ab. Zur Verwendung der NetSEAL-Abfangroutine müssen Sie alle Anwendungen, die die angegebenen Ports verwenden, stoppen und erneut starten. Weitere Informationen über die Verwendung von Policy Director NetSEAL befinden sich im Abschnitt „NetSEAL-Abfangroutine unter AIX verwenden“ auf Seite 72.

Policy Director Authorization ADK konfigurieren

Zum Konfigurieren des Policy Director Authorization ADK klicken Sie auf **Policy Director Authorization ADK** in der Policy Director-Konfigurationsliste.

Die Konfiguration des Policy Director Authorization ADK erfolgt ohne Eingaben des Benutzers.

Policy Director Credentials Acquisition Service konfigurieren

Policy Director CAS wird automatisch installiert. Möchten Sie Policy Director CAS als Ihren Credentials Acquisition Service verwenden, müssen Sie CAS konfigurieren. Informationen über Policy Director CAS und über die Konfiguration von CAS für den WebSEAL-Server befinden sich in dem Handbuch *Policy Director Administration Guide*.

Verwaltungskonsole installieren

Policy Director stellt eine Verwaltungskonsole zur Verfügung, mit der viele Komponenten des Policy Director-Sicherheitssystems von einem Windows-Client-Desktop verwaltet werden. Die Verwaltungskonsole kann unter den folgenden Betriebssystemen installiert werden:

- Windows 95
- Windows 98
- Windows NT Version 4.0 mit Service Pack 4 oder höher
- AIX Version 4.3.1.0 oder höher

Jedes Windows-Betriebssystem, unter dem Policy Director ausgeführt wird, erfordert den Policy Director NetSEAT-Client.

Der NetSEAT-Client kann entweder als DCE-Laufzeit-Client oder als Client für einen Policy Director-Server konfiguriert werden. Obwohl beide Konfigurationen von der Verwaltungskonsole akzeptiert werden, erfordern die Policy Director-Server den vollständigen Client für den Policy Director-Server.

Müssen Komponenten erneut installiert werden, muß die vorhandene Komponente entfernt werden, bevor sie erneut installiert wird.

NetSEAL-Abfangroutine unter AIX verwenden

Um die Policy Director NetSEAL-Abfangroutine zu verwenden, muß der NetSEAL-Dämon Sicherheitsmanager (secmgrd) vor allen Anwendungen gestartet werden, die auf gesicherte (abgefangene) Ports zugreifen. Verwenden Sie /etc/inittab-Einträge, um sicherzustellen, daß während des Startprozesses secmgrd vor den Anwendungen gestartet wird.

Verwenden Sie die NetSEAL-Abfangroutine zusammen mit Netzanwendungen, wie beispielsweise Telnet, RLOGIN und POP3. Der Dämon **inetd** steuert diese Anwendungen. Mit der Policy Director-Startprozedur /etc/iv/iv wird secmgrd gestartet, und dann der Dämon inetd gestoppt und erneut gestartet. Mit dieser Prozedur wird die erfolgreiche Aktivierung der Abfangfunktion für diese Anwendungen nach dem Systemstart gewährleistet.

Wird Policy Director gestoppt und erneut gestartet, müssen Sie auch alle Anwendungen stoppen und erneut starten, die Anforderungen an abgefangene Ports senden. Um diesen Prozeß zu automatisieren, können Sie der Prozedur /etc/iv/iv Code hinzufügen, um die Anwendungen nach dem Start von secmgrd zu stoppen und zu starten. Verwenden Sie die Technik der Prozedur /etc/iv/iv zum Stoppen und erneuten Starten von **inetd** als Schablone zum Stoppen und Starten anderer Anwendungen.

Weitere Informationen über die Konfiguration von Policy Director NetSEAL zum Abfangen von Anforderungen für bestimmte Ports enthalten die Informationen über NetSEAL im Handbuch *Policy Director Administration Guide*.

Policy Director entfernen

Sie müssen Policy Director für AIX dekonfigurieren, bevor Sie Policy Director entfernen können.

- Informationen über die Dekonfiguration von Policy Director befinden sich im Abschnitt „Policy Director-Pakete dekonfigurieren“.
- Informationen über das Entfernen von Policy Director befinden sich im Abschnitt „Policy Director-Pakete entfernen“ auf Seite 74.

Policy Director-Pakete dekonfigurieren

Führen Sie die folgenden Schritte aus, um die Policy Director-Server zu dekonfigurieren:

1. Starten Sie SMIT.
2. Klicken Sie auf **Netzkommunikation und -anwendungen**.
   Das Menü 'Netzkommunikation und -anwendungen' wird angezeigt.
3. Klicken Sie auf **Policy Director**. Das Policy Director-Menü wird angezeigt.
4. Klicken Sie im Menü auf **Policy Director - Dekonfiguration**.
   Die Liste der konfigurierten Policy Director-Pakete wird angezeigt.

   Wählen Sie das Paket aus, das dekonfiguriert werden soll. Folgende Pakete können angezeigt werden:

   - Policy Director-Berechtigungs-Server - Dekonfiguration
   - Policy Director Authorization ADK - Dekonfiguration
   - Policy Director NetSEAL - Dekonfiguration
   - Policy Director WebSEAL - Dekonfiguration
   - Policy Director-Sicherheitsmanager - Dekonfiguration
   - Policy Director-Verwaltungs-Server - Dekonfiguration
   - Policy Director-Verwaltungskonsole - Dekonfiguration
   - Policy Director-Basis - Dekonfiguration
   - IV Smit-Menü - Dekonfiguration
5. Pakete müssen einzeln dekonfiguriert werden.

   Anmerkung: Die Pakete müssen in umgekehrter Reihenfolge wie bei der Installation dekonfiguriert werden. Um diese Reihenfolge sicherzustellen, dekonfigurieren Sie die Pakete von oben nach unten im Menü.
6. Werden Policy Director-Pakete dekonfiguriert, weil Policy Director vollständig von dem Computer entfernt werden soll, klicken Sie auf **Policy Director Smit-Menü - Dekonfiguration**, nachdem Sie alle anderen Policy Director-Pakete dekonfiguriert haben.

   Mit diesem Schritt werden Policy Director-Paketinformationen aus der SMIT-Datenbank entfernt.
7. Lesen Sie den Abschnitt „Policy Director-Pakete entfernen“ auf Seite 74, um Policy Director zu entfernen.

Policy Director-Pakete entfernen

Bevor Sie versuchen, Policy Director zu entfernen, stellen Sie sicher, daß die Policy Director-Software dekonfiguriert wurde. Der Abschnitt „Policy Director-Pakete dekonfigurieren“ auf Seite 73 enthält Anweisungen zur Dekonfiguration.

Gehen Sie wie folgt vor, um Policy Director zu entfernen:

1. Starten Sie SMIT.
2. Klicken Sie auf **Softwareinstallation und Wartung**.

   Das Menü 'Softwareinstallation und Wartung' wird angezeigt.
3. Klicken Sie auf **Softwarewartung und Dienstprogramme**.

   Das Menü 'Softwarewartung und Dienstprogramme' wird angezeigt.
4. Klicken Sie auf **Installierte Software entfernen**.

   Das Fenster 'Installierte Software entfernen' wird angezeigt.
5. Wählen Sie die Policy Director-Pakete aus, die entfernt werden sollen. Sie können mehrere Pakete gleichzeitig auswählen.

   Sollen alle Policy Director-Pakete entfernt werden, geben Sie `IV` ein.

Die Policy Director-Software wird entfernt.

Verwaltungskonsole und NetSEAT entfernen

Die Verwaltungskonsole unter Windows und der NetSEAT-Client unter Windows können mit der Deinstallationsfunktion des InstallShield entfernt werden:

- Verwaltungskonsole entfernen. Der Abschnitt „Verwaltungskonsole entfernen“ auf Seite 57 enthält Anweisungen.
- NetSEAT-Client entfernen. Der Abschnitt „NetSEAT-Client entfernen“ auf Seite 58 enthält Anweisungen.

Installation von Policy Director für Solaris

Die Abschnitte in diesem Kapitel beschreiben die Installation und Konfiguration von Policy Director unter dem Betriebssystem Solaris.

Bevor Sie mit der Installation von Policy Director beginnen, stellen Sie sicher, daß Sie die Informationen in „Vor der Installation von Policy Director für Solaris“ gelesen haben.

Vor der Installation von Policy Director für Solaris

Bevor Sie mit der Installation von Policy Director beginnen, lesen Sie die folgenden Informationen:

Die Installationsprozedur für dieses Release von Policy Director erfordert den Befehl **pkgadd**. Geben Sie folgendes in eine Eingabeaufforderung ein, um den Befehl **pkgadd** auszuführen:

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

Verwenden Sie den Befehl **pkgadd**, um die Policy Director-Software zu installieren. Der Befehl **pkgadd** zeigt häufig weitere Eingabeaufforderungen an, die in den Standardprozeduranweisungen nicht angegeben sind. Diese Eingabeaufforderungen erscheinen als Antwort auf Situationen, die für Ihre Systeminstallation und -konfiguration spezifisch sind. Antworten Sie auf diese Eingabeaufforderungen, die außerhalb der Standardprozeduren angezeigt werden, immer mit `y`.

Bevor Sie Policy Director installieren,

- müssen Sie einen DCE-Client installieren.
- müssen Sie außerdem einen LDAP-Client installieren, wenn Sie LDAP als Benutzerregistrierungsdatenbank verwenden.

Sie müssen die Transarc DCE-Fernverwaltungsfunktionen aktivieren, bevor Sie mit der Installation von Policy Director beginnen. Sie können die Policy Director-Installation nicht ausführen, wenn die Fernverwaltungsfunktionen nicht aktiviert sind.

Die Verwendung einiger Fernverwaltungsfunktionen ermöglicht dem Zellenadministrator im Prinzip die Gleichstellung mit dem Konto des lokalen Roots. Transarc DCE inaktiviert normalerweise diese Fernverwaltungsfunktionen. Diese Funktionen werden jedoch von der Policy Director-Software benötigt.

Der Abschnitt 4.2.1 in *Transarc Release Notes, Release 1.1* (DCE-D1002-01) enthält Informationen über die Aktivierung der Fernverwaltungsfunktionen.

Installationsanzeigenausgabe

Die Standardprozeduren in diesem Dokument geben nicht alle möglichen Anzeigenausgaben des Befehls **pkgadd** an. Die meisten nicht dokumentierten Anzeigenausgaben stellen zusätzliche Informationen über die Operationen zur Verfügung, die gerade ausgeführt werden. Im allgemeinen zeigen die Standardprozeduren in dieser Dokumentation nur die Nachrichten, die eine Benutzeraktion erfordern.

Policy Director-Server mit einer LDAP-Benutzerregistrierungsdatenbank installieren

Installieren Sie Policy Director mit einer DCE-Benutzerregistrierungsdatenbank, fahren Sie mit dem Abschnitt „Policy Director-Server mit einer DCE-Benutzerregistrierungsdatenbank installieren“ auf Seite 83 fort.

Die Server-Pakete befinden sich in dem Verzeichnis /solaris auf der CD *IBM SecureWay Policy Director Version 3.0*.

Sie müssen als Root angemeldet sein, um die Policy Director-Pakete installieren zu können.

Muß ein Paket erneut installiert werden, müssen Sie zuerst das vorhandene Paket (**pkgrm**) entfernen, bevor Sie das gewünschte Paket erneut installieren.

Gehen Sie wie folgt vor, um den Verwaltungs-Server zu installieren:

1. Stellen Sie sicher, daß der LDAP-Server installiert und aktiv ist, wenn LDAP als Benutzerregistrierungsdatenbank verwendet werden soll. Vollständige Anweisungen befinden sich in „Installation und Konfiguration von IBM SecureWay Directory“ auf Seite 29.
2. Geben Sie den Befehl **pkgadd** ein, um die verfügbaren Pakete auf der CD aufzulisten:

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

   Die Liste der verfügbaren Pakete wird angezeigt.

   Verwenden Sie einen anderen Mount-Punkt für die CD-ROM, ersetzen Sie den Mount-Punkt in dem oben genannten Befehl.
3. Geben Sie die Auswahlnummer für IVBase ein, um die Policy Director-Basisdateien zu installieren, und drücken Sie dann die Eingabetaste.

   Mit diesem Befehl werden Dateien aus der CD extrahiert und an der angegebenen Position auf der Festplatte installiert.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVBase-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Bevor Sie mit dem nächsten Schritt fortfahren, beachten Sie, daß nur ein Exemplar des Verwaltungs-Servers (IVMgr) in der gesicherten Domäne vorhanden sein darf. Ist dies eine Installation für ein eigenständiges System, fahren Sie mit dem nächsten Schritt fort. Erfolgt die Installation auf einem sekundären Server, stellen Sie sicher, daß Sie die Informationen im Abschnitt „Installationsvoraussetzungen für die gesicherte Domäne“ auf Seite 23 gelesen haben.

4. Geben Sie die Auswahlnummer für IVMgr ein, um die Dateien für den Policy Director-Verwaltungs-Server zu installieren. Drücken Sie die Eingabetaste.

   Mit diesem Befehl werden Dateien aus der CD extrahiert und an der angegebenen Position auf der Festplatte installiert.

   Es erscheint eine Eingabeaufforderung, in der Sie aufgefordert werden, eine Art der Benutzerregistrierungsdatenbank auszuwählen.

5. Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, geben Sie eine `2` für LDAP-Benutzerregistrierungsdatenbank ein.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

6. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Eine Reihe von Eingabeaufforderungen zum Konfigurieren der Kommunikation zwischen dem Verwaltungs-Server und dem LDAP-Server wird angezeigt.

7. Geben Sie die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:
   - Host-Name des LDAP-Servers
   - Port-Nummer des LDAP-Servers
   - SSL-Port-Nummer des LDAP-Servers

8. Geben Sie den DN und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein (beispielsweise `cn=root`). Der LDAP-Server enthält jetzt Policy Director-Sicherheitsinformationen.

9. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen dem Verwaltungs-Server und dem LDAP-Server.

   Sie können die SSL-Übertragung zwischen jedem Policy Director-Server und dem LDAP-Server individuell aktivieren oder inaktivieren. In diesem Fall wird die SSL-Übertragung zwischen dem Verwaltungs-Server und dem LDAP-Server konfiguriert.

10. Haben Sie die SSL-Übertragung inaktiviert, überspringen Sie diesen Schritt. Wurde die SSL-Übertragung aktiviert, stellen Sie Werte für die folgenden Eingabeaufforderungen zur Verfügung:

    - `Position der SSL-Schlüsseldatei`
    - `SSL-Schlüsselkennsatz`
    - `Kennwort für SSL-Schlüsseldatei`

11. Aktivieren Sie den GSO-Datenbankzugriff, indem Sie den DN für das GSO-Datenbanksuffix zur Verfügung stellen, das Sie in „Suffixe hinzufügen“ auf Seite 30 hinzugefügt haben.

    Beispiel:

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

    Nachdem der GSO-Datenbankzugriff konfiguriert wurde, konfiguriert der Policy Director-Konfigurationsmanager automatisch einen DSB. In einer Reihe von Nachrichten wird jeder automatisierte Schritt bei seiner Beendigung aufgelistet.

    Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVMgr-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Sicherheitsmanager für WebSEAL und NetSEAL installieren

Das Paket mit dem Sicherheitsmanager (IVNet) erfordert Ressourcen aus dem Basispaket. Stellen Sie sicher, daß die Basiskomponente installiert ist, bevor Sie IVNet installieren.

1. Geben Sie die Auswahlnummer für IVNet ein, um die Dateien für den Policy Director-Sicherheitsmanager zu installieren, und drücken Sie die Eingabetaste.

   Dateien werden aus der CD extrahiert und im Standardverzeichnis auf der Festplatte installiert.

   Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, wird eine Reihe von Eingabeaufforderungen zur Integration des Sicherheitsmanagers mit dem LDAP-Server angezeigt.

2. Geben Sie auf Anforderung die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:

   - Host-Name des LDAP-Servers
   - Port-Nummer des LDAP-Servers
   - SSL-Port-Nummer des LDAP-Servers

   Die genannten Eingabeaufforderungen für die LDAP-Server-Konfiguration werden nur angezeigt, wenn die Kommunikation mit dem LDAP-Server noch nicht für andere Policy Director-Pakete auf diesem System konfiguriert wurde. Wurde der Verwaltungs-Server (IVMgr) oder der Berechtigungs-Server (IVAcld) auf diesem System konfiguriert, werden die genannten Eingabeaufforderungen in diesem Schritt nicht angezeigt.

3. Geben Sie den DN und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein.

   Der LDAP-Server enthält jetzt Policy Director-Sicherheitsinformationen.

4. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen dem Sicherheitsmanager und dem LDAP-Server.

   Sie können die SSL-Übertragung zwischen jedem Policy Director-Server und dem LDAP-Server individuell aktivieren oder inaktivieren. In diesem Fall wird die SSL-Übertragung zwischen dem Sicherheitsmanager und dem LDAP-Server konfiguriert.

5. Haben Sie die SSL-Übertragung inaktiviert, überspringen Sie diesen Schritt. Wurde die SSL-Übertragung aktiviert, stellen Sie Werte für die folgenden Eingabeaufforderungen zur Verfügung:

   - `Position der SSL-Schlüsseldatei`
   - `SSL-Schlüsselkennsatz`
   - `Kennwort für SSL-Schlüsseldatei`

6. Aktivieren Sie den GSO-Datenbankzugriff, indem Sie den DN für das GSO-Datenbanksuffix zur Verfügung stellen, das Sie in „Suffixe hinzufügen“ auf Seite 30 hinzugefügt haben.

   Beispiel:

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

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

7. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Der Sicherheitsmanager wird konfiguriert und gestartet.

   Der CAS-Server wird konfiguriert und gestartet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVNet-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

WebSEAL-Komponente aktivieren

Installieren Sie das Paket WebSEAL (IVWeb), wenn die WebSEAL-Komponente aktiviert werden soll.

1. Geben Sie die Auswahlnummer für IVWeb ein, um die Dateien zu installieren, die für die Aktivierung der WebSEAL-HTTP-Server-Komponente erforderlich sind.
2. Drücken Sie die Eingabetaste, um fortzufahren.

   Die Dateien werden aus der CD extrahiert und auf der Festplatte installiert.

   Eine Konfigurationsliste mit Werten wird angezeigt, die den HTTP- und HTTPS-Client-Zugriff, die erforderlichen TCP-Ports und das Standardstammverzeichnis für Web-Dokumente angeben.
3. Bestätigen Sie die aktuellen Konfigurationswerte:

   ```
   Web-Server-Konfiguration überprüfen:
   1. TCP HTTP aktivieren?              Ja
   2. HTTP-Port                         80
   3. HTTPS aktivieren?                 Ja
   4. HTTPS-Port                        443
   5. Web-Dokumentstammverzeichnis      /opt/Policy Director/www/docs

   a. Konfiguration akzeptieren und Installation fortsetzen
   x. Installation verlassen

   Zu ändernden Eintrag auswählen: a
   ```
4. Geben Sie `a` ein, um die Konfiguration zu akzeptieren und die Installation fortzusetzen, und drücken Sie dann die Eingabetaste.
5. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Die Installation konfiguriert und aktiviert WebSEAL auf dem Computer. Der Sicherheitsmanager wird automatisch erneut gestartet.

NetSEAL-Komponente aktivieren

Installieren Sie das Paket NetSEAL (IVTrap), wenn die NetSEAL-Komponente aktiviert werden soll.

1. Geben Sie die Auswahlnummer für IVTrap ein, um die Dateien zu installieren, die für die Aktivierung der grobkörnigen NetSEAL-TCP/IP-Zugriffssteuerung erforderlich sind, und drücken Sie dann die Eingabetaste.

   NetSEAL wird konfiguriert und aktiviert.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   In einer Nachricht wird angegeben, daß Sie unter Verwendung des Befehls **ivadmin** geschützte Ports angeben müssen.

   In einer weiteren Nachricht wird angegeben, daß Sie das System erneut starten müssen (Warmstart), um sicherzustellen, daß alle geschützten Ports unter NetSEAL-Steuerung gestellt werden.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVTrap-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Policy Director NetSEAL fängt Anforderungen an bestimmte Ports ab. Zur Verwendung der NetSEAL-Abfangroutine müssen Sie alle Anwendungen, die die angegebenen Ports verwenden, stoppen und erneut starten. Weitere Informationen über die Konfiguration von Policy Director NetSEAL enthält die Übersicht über NetSEAL im Handbuch *Policy Director Administration Guide.*

Berechtigungs-Server installieren

Gehen Sie wie folgt vor, um den Berechtigungs-Server zu installieren:

1. Geben Sie die Auswahlnummer für IVAcld ein, um die Dateien für den Policy Director-Berechtigungs-Server zu installieren, und drücken Sie dann die Eingabetaste.

   Dateien werden aus der CD extrahiert und im Standardverzeichnis auf der Festplatte installiert.

   Verwenden Sie LDAP als Benutzerregistrierungsdatenbank, wird eine Reihe von Eingabeaufforderungen zur Integration des Berechtigungs-Servers mit dem LDAP-Server angezeigt.

2. Geben Sie auf Anforderung die erforderlichen Informationen für die LDAP-Server-Konfiguration ein:

   - Host-Name des LDAP-Servers
   - Port-Nummer des LDAP-Servers
   - SSL-Port-Nummer des LDAP-Servers

   Die genannten Eingabeaufforderungen für die LDAP-Server-Konfiguration werden nur angezeigt, wenn die Kommunikation mit dem LDAP-Server noch nicht für andere Policy Director-Pakete auf diesem System konfiguriert wurde. Wurde der Verwaltungs-Server (IVMgr) oder der Sicherheitsmanager (IVNet) auf diesem System konfiguriert, werden die genannten Eingabeaufforderungen in diesem Schritt nicht angezeigt.

3. Geben Sie den DN und das Kennwort für den LDAP-Benutzer mit Verwaltungsaufgaben ein.

   Der LDAP-Server enthält jetzt Policy Director-Sicherheitsinformationen.

4. Aktivieren oder inaktivieren Sie die SSL-Übertragung zwischen dem Verwaltungs-Server und dem LDAP-Server.

   Sie können die SSL-Übertragung zwischen jedem Policy Director-Server und dem LDAP-Server individuell aktivieren oder inaktivieren. In diesem Fall wird die SSL-Übertragung zwischen dem Verwaltungs-Server und dem LDAP-Server konfiguriert.

5. Haben Sie die SSL-Übertragung inaktiviert, überspringen Sie diesen Schritt. Wurde die SSL-Übertragung aktiviert, stellen Sie Werte für die folgenden Eingabeaufforderungen zur Verfügung:

   - `Position der SSL-Schlüsseldatei`
   - `SSL-Schlüsselkennsatz`
   - `Kennwort für SSL-Schlüsseldatei`

6. Aktivieren Sie den GSO-Datenbankzugriff, indem Sie den DN für das GSO-Datenbanksuffix zur Verfügung stellen, das Sie in „Suffixe hinzufügen“ auf Seite 30 hinzugefügt haben.

   Beispiel:

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

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

7. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Der Berechtigungs-Server wird konfiguriert und gestartet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVAcld-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Berechtigungs-API-Komponente installieren

Geben Sie die Auswahlnummer für IVAuthADK ein, um die Berechtigungs-API für C-Dateien zu installieren, und drücken Sie dann die Eingabetaste.

Dateien werden aus der CD extrahiert und im Standardverzeichnis auf der Festplatte installiert.

Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVAuthADK-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Policy Director-Server mit einer DCE-Benutzerregistrierungsdatenbank installieren

Installieren Sie Policy Director mit einer LDAP-Benutzerregistrierungsdatenbank, fahren Sie mit dem Abschnitt „Policy Director-Server mit einer LDAP-Benutzerregistrierungsdatenbank installieren“ auf Seite 76 fort.

Die Server-Pakete befinden sich in dem Verzeichnis /solaris auf der CD *IBM SecureWay Policy Director Version 3.0*.

Sie müssen als Root angemeldet sein, um die Policy Director-Pakete installieren zu können.

Muß ein Paket erneut installiert werden, müssen Sie zuerst das vorhandene Paket (**pkgrm**) entfernen, bevor Sie das gewünschte Paket erneut installieren.

Gehen Sie wie folgt vor, um den Verwaltungs-Server zu installieren:

1. Geben Sie den Befehl **pkgadd** ein, um die verfügbaren Pakete auf der CD aufzulisten:

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

   Die Liste der verfügbaren Pakete wird angezeigt.

   Verwenden Sie einen anderen Mount-Punkt für die CD-ROM, ersetzen Sie den Mount-Punkt in dem oben genannten Befehl.

2. Geben Sie die Auswahlnummer für IVBase ein, um die Policy Director-Basisdateien zu installieren, und drücken Sie dann die Eingabetaste.

   Mit diesem Befehl werden Dateien aus der CD extrahiert und an der angegebenen Position auf der Festplatte installiert.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVBase-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

   Bevor Sie mit dem nächsten Schritt fortfahren, beachten Sie, daß nur ein Exemplar des Verwaltungs-Servers (IVMgr) in der gesicherten Domäne vorhanden sein darf. Ist dies eine Installation für ein eigenständiges System, fahren Sie mit dem nächsten Schritt fort. Erfolgt die Installation auf einem sekundären Server, stellen Sie sicher, daß Sie die Informationen im Abschnitt „Installationsvoraussetzungen für die gesicherte Domäne“ auf Seite 23 gelesen haben.

3. Geben Sie die Auswahlnummer für IVMgr ein, um die Dateien für den Policy Director-Verwaltungs-Server zu installieren. Drücken Sie die Eingabetaste. Mit diesem Befehl werden Dateien aus der CD extrahiert und an der angegebenen Position auf der Festplatte installiert.

   Es erscheint eine Eingabeaufforderung, in der Sie aufgefordert werden, eine Art der Benutzerregistrierungsdatenbank auszuwählen.

4. Verwenden Sie DCE als Benutzerregistrierungsdatenbank, geben Sie eine `1` ein.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

5. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVMgr-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Sicherheitsmanager für WebSEAL und NetSEAL installieren

Das Paket mit dem Sicherheitsmanager (IVNet) erfordert Ressourcen aus dem Basispaket. Stellen Sie sicher, daß die Basiskomponente installiert ist, bevor Sie IVNet installieren.

1. Geben Sie die Auswahlnummer für IVNet ein, um die Dateien für den Policy Director-Sicherheitsmanager zu installieren, und drücken Sie die Eingabetaste.

   Dateien werden aus der CD extrahiert und im Standardverzeichnis auf der Festplatte installiert. Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Der Sicherheitsmanager wird konfiguriert und gestartet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVNet-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

WebSEAL-Komponente aktivieren

Installieren Sie das Paket WebSEAL (IVWeb), wenn die WebSEAL-Komponente aktiviert werden soll.

1. Geben Sie die Auswahlnummer für IVWeb ein, um die Dateien zu installieren, die für die Aktivierung der WebSEAL-HTTP-Server-Komponente erforderlich sind.
2. Drücken Sie die Eingabetaste, um fortzufahren. Die Dateien werden aus der CD extrahiert und auf der Festplatte installiert.

   Eine Konfigurationsliste mit Werten wird angezeigt, die den HTTP- und HTTPS-Client-Zugriff, die erforderlichen TCP-Ports und das Standardstammverzeichnis für Web-Dokumente angeben.

3. Bestätigen Sie die aktuellen Konfigurationswerte:

```
Web-Server-Konfiguration überprüfen:
1. TCP HTTP aktivieren?              Ja
2. HTTP-Port                         80
3. HTTPS aktivieren?                 Ja
4. HTTPS-Port                        443
5. Web-Dokumentstammverzeichnis      /opt/Policy Director/www/docs

a. Konfiguration akzeptieren und Installation fortsetzen
x. Installation verlassen

Zu ändernden Eintrag auswählen: a
```

4. Geben Sie `a` ein, um die Konfiguration zu akzeptieren und die Installation fortzusetzen, und drücken Sie dann die Eingabetaste.
5. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

```
Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
Das Kennwort des Zellenadministrators eingeben:
```

   Die Installation konfiguriert und aktiviert WebSEAL auf dem Computer. Der Sicherheitsmanager wird automatisch erneut gestartet.

NetSEAL-Komponente aktivieren

Installieren Sie das Paket NetSEAL (IVTrap), wenn die NetSEAL-Komponente aktiviert werden soll.

1. Geben Sie die Auswahlnummer für IVTrap ein, um die Dateien zu installieren, die für die Aktivierung der grobkörnigen NetSEAL-TCP/IP-Zugriffssteuerung erforderlich sind, und drücken Sie dann die Eingabetaste.

   NetSEAL wird konfiguriert und aktiviert.

   Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.
2. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   In einer Nachricht wird angegeben, daß Sie unter Verwendung des Befehls **ivadmin** geschützte Ports angeben müssen.

In einer weiteren Nachricht wird angegeben, daß Sie das System erneut starten müssen (Warmstart), um sicherzustellen, daß alle geschützten Ports unter NetSEAL-Steuerung gestellt werden.

Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVTrap-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Policy Director NetSEAL fängt Anforderungen an bestimmte Ports ab. Zur Verwendung der NetSEAL-Abfangroutine müssen Sie alle Anwendungen, die die angegebenen Ports verwenden, stoppen und erneut starten. Weitere Informationen über die Konfiguration von Policy Director NetSEAL enthält die Übersicht über NetSEAL im Handbuch *Policy Director Administration Guide.*

Berechtigungs-Server installieren

Gehen Sie wie folgt vor, um den Berechtigungs-Server zu installieren:

1. Geben Sie die Auswahlnummer für IVAcld ein, um die Dateien für den Policy Director-Berechtigungs-Server zu installieren, und drücken Sie dann die Eingabetaste.

   Dateien werden aus der CD extrahiert und im Standardverzeichnis auf der Festplatte installiert. Eine Eingabeaufforderung erscheint, in der Sie aufgefordert werden, den Namen und das Kennwort des DCE-Zellenadministrators einzugeben.

2. Geben Sie die erforderlichen Informationen für den Zugriff auf das DCE-Zellenadministratorkonto ein.

   ```
   Den Benutzernamen des Zellenadministrators [cell_admin] eingeben:
   Das Kennwort des Zellenadministrators eingeben:
   ```

   Der Berechtigungs-Server wird konfiguriert und gestartet.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVAcld-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Berechtigungs-API-Komponente installieren

Geben Sie die Auswahlnummer für IVAuthADK ein, um die Berechtigungs-API für C-Dateien zu installieren, und drücken Sie dann die Eingabetaste.

Dateien werden aus der CD extrahiert und im Standardverzeichnis auf der Festplatte installiert.

Eine Nachricht wird angezeigt, in der die erfolgreiche Installation des IVAuthADK-Pakets angegeben ist. Die Liste mit den verfügbaren Paketen wird erneut angezeigt.

Credentials Acquisition Service konfigurieren

Policy Director CAS wird automatisch installiert. Möchten Sie Policy Director CAS als Ihren Credentials Acquisition Service verwenden, müssen Sie CAS konfigurieren. Die Informationen über die Konfiguration eines Credentials Acquisition Service im Handbuch *Policy Director Administration Guide* enthalten Anweisungen.

Verwaltungskonsole installieren

Policy Director stellt eine Verwaltungskonsole zur Verfügung, mit der viele Policy Director-Komponenten verwaltet werden.

Die Verwaltungskonsole für Solaris wird unter Verwendung des IVConsole-Installationspakets installiert. Verwenden Sie **pkgadd**, um das Paket zu installieren und zu konfigurieren.

1. Melden Sie sich als Root an.
2. Legen Sie die CD *IBM SecureWay Policy Director Version 3.0* in das CD-ROM-Laufwerk des Policy Director-Server-Systems ein.
3. Rufen Sie die Liste der verfügbaren Pakete auf:

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

4. Geben Sie die Auswahlnummer für IVBase ein, wenn das Paket noch nicht installiert ist. Ist IVBase bereits installiert, fahren Sie mit Schritt 6 fort.
5. Geben Sie `y` ein, um fortzufahren. Die Liste der Pakete wird angezeigt.
6. Geben Sie die Auswahlnummer für IVConsole ein.
7. Geben Sie `y` ein, um fortzufahren.

   Eine Nachricht wird angezeigt, in der die erfolgreiche Installation angegeben ist. Die Verwaltungskonsole kann jetzt gestartet werden.

Verwaltungskonsole starten

Gehen Sie wie folgt vor, um die Verwaltungskonsole zu starten:

1. Stellen Sie sicher, daß die Policy Director-Server installiert und aktiv sind.
2. Geben Sie den folgenden Befehl ein:

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

Policy Director entfernen

Entfernen Sie die Policy Director-Server von dem Computer, indem Sie das Dienstprogramm **pkgrm** verwenden. Die Pakete müssen in umgekehrter Reihenfolge wie bei der Installation entfernt werden. Die Befehle **pkgrm** und **pkgadd** sind Member derselben Dienstprogrammfamilie und verfügen über dieselbe Benutzerschnittstelle. Der Root führt das Dienstprogramm **pkgrm** aus.

Es gibt mehrere Methoden für die Verwendung dieses Befehls:

- Starten Sie den Befehl **pkgrm** ohne Argumente.

  Eine numerierte Liste der aktuellen Pakete auf Ihrem Computer wird angezeigt. Geben Sie eine einzelne Auswahlnummer für das Paket ein, das entfernt werden soll.

- Starten Sie den Befehl **pkgrm** und geben Sie einen einzelnen Paketnamen als Argument für den Befehl an. Beispiel:

  ```
  # pkgrm IVBase
  ```

- Starten Sie den Befehl **pkgrm** und geben Sie eine Folge von Paketnamen als Argumente für den Befehl an. Beispiel:

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

Ausführliche Informationen über den Befehl **pkgrm** befinden sich in der Dokumentation zum Betriebssystem Solaris.

Anmerkung: Sie müssen die Policy Director-Pakete in exakt umgekehrter Reihenfolge wie bei der Installation entfernen.

Gehen Sie wie folgt vor, um Policy Director zu entfernen:

1. Melden Sie sich als Root bei dem Solaris-Betriebssystem an.

   Verwenden Sie eine der genannten Methoden zum Starten des Befehls **pkgrm**.

2. Policy Director-Komponenten müssen in der folgenden Reihenfolge entfernt werden:

   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

   Die Konfiguration Ihres Datenverarbeitungssystems enthält möglicherweise nicht alle Pakete, die in der vorherigen Liste aufgeführt sind. Die Policy Director-Verwaltungskonsole (IVConsole) kann jederzeit vor dem Paket IVBase entfernt werden.

Verwaltungskonsole entfernen

Gehen Sie wie folgt vor, um die Verwaltungskonsole zu entfernen:

1. Melden Sie sich als Root an.
2. Geben Sie den folgenden Befehl ein:

   ```
   # pkgrm ivconsole
   ```

Referenzliteratur

In der in diesem Kapitel aufgelisteten Dokumentation können Sie weitere Informationen über Policy Director Version 3.0 und über die zugehörigen Produkte finden.

Dokumentation zu Policy Director

Dieses Handbuch, *IBM SecureWay Policy Director Installation und Konfiguration, Version 3.0*, wird nicht nur zusammen mit dem Policy Director-Produkt, sondern auch in einem Dokumentationspaket zur Verfügung gestellt. Das Dokumentationspaket für Policy Director enthält dieses Handbuch und die Policy Director-Lizenzinformation.

Zusätzlich zu diesem Handbuch enthalten die folgenden Dokumentationen Informationen über Policy Director. Sie sind im PDF-Format (PDF = PostScript Document Format) verfügbar und befinden sich im Unterverzeichnis /doc auf der CD *IBM SecureWay Policy Director Version 3.0*.

- *IBM SecureWay Policy Director Administration Guide, Version 3.0*

  Dieses Handbuch enthält ausführliche Anweisungen zur Verwaltung von Policy Director. Das Handbuch stellt unter anderem folgende Informationen über IBM SecureWay Policy Director zur Verfügung:

  – Policy Director-Konzepte, wie beispielsweise Authentifizierung, Berechtigung und Berechtigungsakquisition
  – Allgemeine Verwaltungs-Tasks unter Verwendung der Verwaltungskonsole
  – WebSEAL-Verwaltung
  – NetSEAL-Verwaltung
  – NetSEAT-Verwaltung
  – Verwaltungsressourcen (Befehl **ivadmin**)

- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

  Dieses Handbuch beschreibt die Berechtigungs-API-Komponenten und die Ausführung der folgenden Tasks:

  – Erstellen von Anwendungen mit der Berechtigungs-API
  – Initialisieren des Policy Director-Berechtigungsservices
  – Authentifizieren eines Anwendungs-Servers oder Clients
  – Erwerben von Benutzerberechtigungen
  – Treffen einer Berechtigungsentscheidung
  – Ausführen wahlfreier Tasks
  – Bereinigen und Systemabschluß durchführen
  – Einsetzen von Anwendungen mit der Berechtigungs-API

Die Policy Director-Informationsdatei enthält möglicherweise die neuesten Informationen über Policy Director, die die Informationen in den Produktveröffentlichungen ersetzen.

Soll die neueste Informationsdatei angefordert werden, auf die Bibliotheksseite der IBM SecureWay Policy Director Web-Site zugreifen.

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

Dokumentation zu IBM SecureWay FirstSecure

Das folgende Handbuch enthält Informationen über FirstSecure:

- *IBM SecureWay FirstSecure Planung und Integration, Version 2.0 (CT7EHDE)*

  Dieses Handbuch beschreibt FirstSecure und die Produkte, die zu FirstSecure gehören, und hilft bei der Planung der Verwendung aller IBM SecureWay-Produkte.

IBM SecureWay Policy Director (Policy Director) ist entweder als Komponente von IBM SecureWay FirstSecure oder als eigenständiges Produkt verfügbar. Ist Ihre Version von Policy Director im FirstSecure-Angebot enthalten, wird dieses Handbuch mit FirstSecure zur Verfügung gestellt. Haben Sie Ihre Version von Policy Director als eigenständiges Produkt erworben, befindet sich dieses Handbuch auf der folgenden FirstSecure Web-Seite:

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

Dokumentation zu IBM Distributed Computing Environment

Die folgenden Dokumentationen beschreiben die Installation von DCE. Sie befinden sich im PDF-Format auf der CD *IBM SecureWay Policy Director Security Services* unter /doc oder auf der folgenden DCE Web-Site:

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

IBM DCE für Windows NT

Einstieg in IBM Distributed Computing Environment für Windows NT Version 2.2 kann über folgende Web-Adresse aufgerufen werden:

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

Dieses Handbuch beschreibt Distributed Computing Environment (DCE) für Windows NT, Version 2.2, sowie die Planung, Installation und Konfiguration des Produkts.

Das Handbuch *Einstieg in IBM Distributed Computing Environment für Windows NT Version 2.2* befindet sich auch auf der CD *IBM SecureWay Policy Director Security Services* in /doc/DCE22_QuickBeginnings_NT.pdf.

IBM DCE für AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2 kann über folgende Web-Adresse aufgerufen werden:

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

Dieses Handbuch beschreibt IBM Distributed Computing Environment für AIX, Version 2.2 (DCE 2.2 für AIX), sowie die Planung, Installation und Konfiguration des Produkts.

Das Handbuch *IBM Distributed Computing Environment for AIX Quick Beginnings Version 2.2* befindet sich auch auf der CD *IBM SecureWay Policy Director Security Services* in /doc/DCE22_QuickBeginnings_AIX.pdf.

Transarc DCE für Solaris

Die Dokumentationen *Transarc DCE Version 2.0 Release Notes* und *Installation and Configuration Guide* können über folgende Web-Adresse aufgerufen werden:

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

Die *Transarc DCE Version 2.0 Release Notes* dokumentieren die folgenden Informationen über Transarc DCE-Software und -Dokumentation:

- Unterschiede zwischen OSF DCE und dem Produkt DCE * DFS
- Unterschiede zwischen Version 2.0 und Version 1.1 von DCE * DFS
- Bekannte Fehler und Einschränkungen in DCE * DFS

Die *Transarc DCE Version 2.0 Release Notes* befinden sich auch auf der CD *IBM SecureWay Policy Director Security Services* in /doc/DCE20_ReleaseNotes_Solaris.pdf.

Das Handbuch *Installation and Configuration Guide* enthält Anweisungen zur Installation, Konfiguration und Aufrüstung des Produkts DCE DFS 2.0.

Das Handbuch *Installation and Configuration Guide* befindet sich auch auf der CD *IBM SecureWay Policy Director Security Services* in /doc/DCE20_InstallGuide_Solaris.pdf.

Dokumentation zu IBM SecureWay Directory

Das folgende Handbuch enthält Installations- und Konfigurationsinformationen für IBM SecureWay Directory (LDAP):

- *IBM SecureWay Directory Installations- und Konfigurationshandbuch, Version 3.1.1*

  Für alle unterstützten Betriebssysteme ist eine separate Version dieses Handbuchs in HTML-Format vorhanden. Das Handbuch für jedes Betriebssystem befindet sich auf der entsprechenden CD unter /doc/wparent.htm. Die CDs sind:

  – *IBM SecureWay Directory Version 3.1.1 für NT*

  – *IBM SecureWay Directory Version 3.1.1 für AIX*

  – *IBM SecureWay Directory Version 3.1.1 für Solaris*

  Nach der LDAP-Installation befindet sich die .HTM-Dokumentationsdatei mit den Installations- und Konfigurationsinformationen unter:

  `C:\Programmdateien\IBM\LDAP\nls\html\enUS1252\config\wparent.htm`

Das folgende Handbuch als HTML-Datei enthält Informationen über die Verwaltung von IBM SecureWay:

- *IBM SecureWay Directory Administration Guide, Version 3.1.1*

  1. Nach einer Standardinstallation von LDAP können Sie mit einem Web-Browser auf die Dokumentation zugreifen, die sich an folgender Position befindet:

     `C:\Programmdateien\IBM\LDAP\nls\html\enUS1252\config\wparent.ht`

Das folgende Handbuch in HTML-Format enthält Informationen über den IBM SecureWay Directory-Client:

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

  Dieses Handbuch enthält Links zu folgenden LDAP-Informationen:

  – LDAP Client SDK Plugin Programming Reference

    1. Nach einer Standardinstallation von LDAP können Sie mit einem Web-Browser auf die Dokumentation zugreifen, die sich an folgender Position befindet:

       `C:\Programmdateien\IBM\doc\progref.htm`

    2. Öffnen Sie die Dokumentation *IBM SecureWay Directory Client SDK Programming Reference*.
    3. Klicken Sie auf **Appendices**.
    4. Klicken Sie auf **LDAP Client SDK Plugin Programming Reference**

  – Informationen über die Verwendung des GSKit und des Key Management Tools **ikmguiw** zur Konfiguration des LDAP-Servers für die Unterstützung des SSL-Zugriffs

    1. Ist dieses Handbuch noch nicht geöffnet, öffnen Sie die Dokumentation *IBM SecureWay Directory Client SDK Programming Reference*.
    2. Klicken Sie auf **API categories**.
    3. Klicken Sie auf **SSL**.
    4. Klicken Sie auf **LDAP_SSL API**.
    5. Lokalisieren Sie und klicken Sie auf den Link **Using IKMGUI**, um die entsprechende HTML-Datei zu öffnen.

Die folgende Dokumentation ist auch für den IBM SecureWay Directory-Server verfügbar:

- *IBM SecureWay Directory Server Plug-ins Reference*

Anhang A. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an

IBM Europe,
Director of Licensing,
92066 Paris La Defense Cedex,
France,
zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Web-Sites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Web-Sites dar. Das über diese Web-Sites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Web-Sites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne daß eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden, Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape und die Netscape-Logos	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Java und alle auf Java basierenden Marken und Logos sind Marken von Sun Microsystems Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Index

C

D

E

F

G

H

I

J

K

L

M

N

P

R

S

T

U

V

W

Z

Antwort

IBM SecureWay Policy Director
Installation und Konfiguration
Version 3 Release 0

IBM Teilenummer CT63KDE

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen.
Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Senden Sie Ihre Anregungen bitte an die angegebene Adresse.

IBM Deutschland
Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Kommentare:

Zu Ihrer weiteren Information:

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre *IBM Geschäftsstelle*, Ihren *IBM Geschäftspartner* oder Ihren *Händler*. Unsere Telefonauskunft **„Hallo IBM“** (Telefonnr.: 0180 3/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Teilenummer: CT63KDE

Printed in Denmark

CT63KDE