



Sun Java™ System

Sun Java Enterprise System 5 Guía de actualización para UNIX

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
EE.UU.

Número de referencia: 819-6553-10
Marzo de 2007

Copyright © 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, EE.UU. Todos los derechos reservados.

Sun Microsystems, Inc. tiene derechos de propiedad intelectual relacionados con la tecnología del producto que se describe en este documento. Especialmente, aunque sin limitarse a ello, estos derechos de propiedad intelectual pueden incluir una o varias patentes en los Estados Unidos, las cuales figuran en <http://www.sun.com/patents>, así como una o varias patentes adicionales (o patentes pendientes de adjudicación) en los Estados Unidos y en otros países.

ESTE PRODUCTO CONTIENE INFORMACIÓN CONFIDENCIAL Y SECRETOS COMERCIALES DE SUN MICROSYSTEMS, INC. EL USO, LA REVELACIÓN O LA REPRODUCCIÓN DE DICHOS DATOS ESTÁN PROHIBIDOS SIN EL EXPRESO CONSENTIMIENTO PREVIO Y POR ESCRITO DE SUN MICROSYSTEMS, INC.

Derechos del Gobierno de los EE.UU.: software comercial. Los usuarios gubernamentales están sujetos al acuerdo de licencia estándar de Sun Microsystems, Inc. y a las disposiciones aplicables de la regulación FAR y sus suplementos.

Esta distribución puede incluir materiales desarrollados por terceras partes.

Determinadas partes del producto pueden proceder de sistemas Berkeley BSD, con licencia de la Universidad de California. UNIX es una marca comercial registrada en EE.UU. y en otros países, cuya licencia se otorga exclusivamente a través de X/Open Company, Ltd.

Sun, Sun Microsystems, el logotipo de Sun, Java, Solaris, JDK, Java Naming and Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet y los logotipos de Duke, de Java Coffee Cup, de Solaris, de SunTone Certified y de Sun ONE son marcas comerciales o marcas comerciales registradas de Sun Microsystems, Inc. en EE.UU. y otros países.

Todas las marcas comerciales de SPARC se utilizan bajo licencia y son marcas comerciales o marcas registradas de SPARC International, Inc. en EE.UU. y en otros países. Los productos que llevan la marca comercial SPARC están basados en arquitecturas desarrolladas por Sun Microsystems, Inc.

Legato y el logotipo de Legato son marcas comerciales registradas y Legato NetWorker es una marca comercial o una marca comercial registrada de Legato Systems, Inc. El logotipo de Netscape Communications Corp es una marca comercial o una marca comercial registrada de Netscape Communications Corporation.

La interfaz gráfica de usuario de OPEN LOOK y Sun(TM) fue desarrollada por Sun Microsystems, Inc. para sus usuarios y licenciarios. Sun reconoce los esfuerzos pioneros de Xerox en la investigación y desarrollo del concepto de interfaces gráficas o visuales de usuario para el sector de la informática. Sun dispone de una licencia no exclusiva de Xerox para la interfaz gráfica de usuario de Xerox, que también cubre a los licenciarios de Sun que implementen las GUI de OPEN LOOK y que, por otra parte, cumplan con los acuerdos de licencia por escrito de Sun.

Los productos que se tratan y la información contenida en este manual de servicio están controlados por las leyes de control de exportación de los Estados Unidos y pueden estar sujetos a leyes de exportación o importación en otros países. Queda terminantemente prohibido el uso final (directo o indirecto) de esta documentación para el desarrollo de armas nucleares, químicas, biológicas, de uso marítimo nuclear o misiles. Queda terminantemente prohibida la exportación o reexportación a países sujetos al embargo de los Estados Unidos o a entidades identificadas en las listas de exclusión de exportación de los Estados Unidos, incluidas, aunque sin limitarse a ellas, las personas con acceso denegado y las listas de ciudadanos designados con carácter especial.

ESTA DOCUMENTACIÓN SE PROPORCIONA "TAL COMO ESTÁ" Y NO SE ASUMIRÁ LA RESPONSABILIDAD DE NINGUNA CONDICIÓN EXPRESA O IMPLÍCITA, NI DE REPRESENTACIONES NI GARANTÍAS, INCLUIDA CUALQUIER GARANTÍA IMPLÍCITA DE APROVECHAMIENTO, IDONEIDAD PARA UN FIN PARTICULAR O NO INFRACCIÓN, EXCEPTO EN EL CASO EN QUE TALES RENUNCIAS DE RESPONSABILIDAD NO SE CONSIDEREN LEGALMENTE VÁLIDAS.

Contenido

Lista de tablas	17
Prefacio	21
Público objetivo de este libro	22
Convenciones utilizadas en este libro	22
Interfaces administrativas	22
Convenciones tipográficas	23
Símbolos	23
Indicadores de intérprete de comandos	24
Documentación relacionada	24
Guías incluidas en este conjunto de documentación de Java ES	25
Cómo buscar documentación sobre productos de Sun	26
Acceso en línea a recursos de Sun	27
Contacto con el servicio técnico de Sun	27
Referencias a sitios web de terceros	27
Sun valora sus comentarios	28
 Capítulo1 Planificación de las actualizaciones	29
Componentes de Java ES 5	30
Componentes de productos de la Versión 5	30
Componentes compartidos de la Versión 5	31
Tecnologías de actualización de Java ES	33
Actualización de componentes de productos	33
Enfoques de actualización de los componentes de productos	34
Enfoque de actualización utilizado para cada componente de producto	36
Actualización de los componentes compartidos	38
El proceso de actualización	38
Consideraciones sobre el plan de actualización	40
Dependencias de actualización	40
Estrategias y rutas de actualización admitidas	41

Actualización selectiva o actualización completa	44
Actualización de varias instancias	45
Consideraciones sobre el sistema operativo	46
Revisiones del sistema operativo necesarias	46
Actualizaciones dobles: El software de Java ES y el sistema operativo	46
Actualización del sistema operativo	47
Entornos multizona de Solaris 10	48
Dependencias de los componentes de Java ES	48
Dependencias con componentes compartidos	48
Dependencias con componentes de productos	52
Directrices generales de secuenciación	57
Casos especiales	61
Actualización selectiva: no se actualiza Application Server	61
Actualización de Portal Server de la Versión intermedia (IFR) 7.0 a Java ES 5	62
Actualización a Java ES 5 y zonas de Solaris 10	62
Compatibilidad con las zonas en el programa de instalación de Java ES	62
Actualización de los componentes de productos	63
Sincronice todos los componentes compartidos	64
Procedimientos de actualización recomendados	65
Casos especiales o excepciones	66
Casos especiales de los componentes de productos	66
Casos especiales de los componentes compartidos	66
 Capítulo2 Actualización de los componentes compartidos de Java ES	 69
Visión general de la actualización de componentes compartidos	70
Consideraciones generales	70
Sincronización de los componentes compartidos	70
Sincronización de todos los componentes compartidos	72
Consideraciones de la zona Solaris 10	72
Enfoques para la actualización de componentes compartidos	73
Procedimiento de actualización de componentes compartidos	75
Procedimientos especiales de actualización	75
Procedimientos de actualización de JAVA SE	76
Comprobación del enlace simbólico de Java SE	77
Verificación de la versión actual de Java SE	77
Procedimientos de actualización del contenedor de agentes común	78
 Capítulo3 Software de Sun Cluster	 81
Visión general de la actualización del software de Sun Cluster	82
Acerca del software de Sun Cluster de la Versión 5	82
Guía de actualización del software de Sun Cluster	83
Datos de Sun Cluster	84

Estrategia de actualización para Sun Cluster	85
Problemas de compatibilidad	85
Sun ClusterDependencias	85
Actualización del software de Sun Cluster a Java ES Versión 5	86
Introducción	86
Actualización de Sun Cluster	87
Tareas previas a la actualización	87
Actualización del software de Sun Cluster	91
Verificación de la actualización	92
Tareas posteriores a la actualización	92
Anulación de la actualización	93
 Capítulo4 Sun Cluster Geographic Edition	95
Visión general de las actualizaciones de Sun Cluster Geographic Edition	96
Acerca de Java ES Versión 5	96
Guía de actualización deJava ES Versión 5	96
Datos de Sun Cluster Geographic Edition	97
Estrategia de actualización de Sun Cluster Geographic Edition	97
Problemas de compatibilidad	97
Dependencias	98
Actualización de Sun Cluster Geographic Edition desde la Versión 3.1 8/05	98
Introducción	98
Actualización de la Version 3.1 8/05 de Sun Cluster Geographic Edition	99
Tareas previas a la actualización	99
Actualización de la Versión 3.1 8/05 de Sun Cluster Geographic Edition	102
Verificación de la actualización	105
Tareas posteriores a la actualización	105
Anulación de la actualización	105
 Capítulo5 Directory Server	107
Visión general de la actualización de Directory Server	109
Acerca de Java ES Versión 5	109
Guía de actualización deJava ES Versión 5	109
Datos de Directory Server	111
Estrategia de actualización para Directory Server	112
Problemas de compatibilidad	112
Dependencias	112
Actualización de Directory Server desde Java ES Versión 4	114
Introducción	114
Actualización de la Versión 4 de Directory Server	115
Tareas previas a la actualización	115
Actualización de la Versión 4 de Directory Server	116

Verificación de la actualización	121
Tareas posteriores a la actualización	122
Anulación de la actualización	122
Actualización de varias instancias	122
Actualización por turnos de réplicas de Directory Server	123
Actualización de Directory Server como servicio de datos	123
Actualización de Directory Server desde Java ES Versión 3	123
Actualización de Directory Server desde Java ES Versión 2	123
Capítulo6 Directory Proxy Server	125
Visión general de las actualizaciones de Directory Proxy Server	127
Acerca de Java ES Versión 5	127
Guía de actualización de Java ES Versión 5	127
Datos de Directory Proxy Server	129
Estrategia de actualización para Directory Proxy Server	129
Problemas de compatibilidad	130
Dependencias	131
Actualización de Directory Proxy Server desde Java ES Versión 4	132
Introducción	132
Actualización de la Versión 4 de Directory Proxy Server	133
Tareas previas a la actualización	133
Actualización de la Versión 4 de Directory Proxy Server	134
Verificación de la actualización	137
Tareas posteriores a la actualización	137
Anulación de la actualización	138
Actualización de varias instancias	138
Actualización de Directory Proxy Server desde Java ES Versión 3	139
Actualización de Directory Proxy Server desde Java ES Versión 2	140
Capítulo7 Web Server	141
Visión general de la actualización de Web Server	142
Acerca de Web Server de Java ES Versión 5	142
Guía de actualización de Web Server	143
Datos de Web Server	143
Estrategia de actualización para Web Server	144
Problemas de compatibilidad	144
Web Server Dependencias	145
Actualización de Web Server desde Java ES Versión 4	146
Introducción	146
Actualización de la Versión 4 de Web Server	147
Tareas previas a la actualización	147
Actualización de la Versión 4 de Web Server	148

Verificación de la actualización	162
Tareas posteriores a la actualización	163
Anulación de la actualización	166
Actualización de Web Server desde Java ES Versión 3	168
Actualización de Web Server desde Java ES Versión 2	169
 Capítulo8 Java DB	171
Visión general de las actualizaciones de Java DB	172
Acerca de Java ES Versión 5	172
Guía de actualización deJava ES Versión 5	172
Datos de Java DB	173
Estrategia de actualización para Java DB	173
Problemas de compatibilidad	173
Dependencias	173
Actualización de Java DB desde Java ES Versión 4	174
Introducción	174
Actualización de la Versión 4 de Java DB	174
Tareas previas a la actualización	175
Actualización de la Versión 4 de Java DB	176
Verificación de la actualización	177
Tareas posteriores a la actualización	178
Anulación de la actualización	178
Actualización de varias instancias	178
 Capítulo9 Almacén de sesión de alta disponibilidad	179
Visión general de la actualización de HADB	181
Acerca de HADB de Java ES Versión 5	181
Guía de actualización de HADB	181
Datos de HADB	182
Estrategia de actualización para HADB	182
Problemas de compatibilidad	182
HADBDependencias	183
Actualización de HADB desde Java ES Versión 4	184
Introducción	184
Actualización de la Versión 4 de HADB	185
Tareas previas a la actualización	185
Actualización de la Versión 4 de HADB	186
Verificación de la actualización	189
Tareas posteriores a la actualización	190
Anulación de la actualización	191
Actualización de HADB desde Java ES Versión 3	192

Capítulo10 Message Queue	193
Visión general de la actualización de Message Queue	194
Acerca de Message Queue de Java ES Versión 5	194
Guía de actualización de Message Queue	195
Datos de Message Queue	196
Estrategia de actualización para Message Queue	197
Problemas de compatibilidad	197
Message QueueDependencias	197
Actualización de Message Queue desde Java ES Versión 4	199
Introducción	199
Actualización de la Versión 4 de Message Queue	200
Tareas previas a la actualización	200
Actualización de la Versión 4 de Message Queue	202
Verificación de la actualización de Message Queue	203
Tareas posteriores a la actualización	203
Anulación de la actualización	204
Actualización de varias instancias	205
Actualización de Message Queue desde Java ES Versión 3	206
Actualización de Message Queue desde Java ES Versión 2	207
Introducción	207
Problemas de compatibilidad con la Versión 2	208
Compatibilidad con los protocolos	208
Compatibilidad del agente	208
Compatibilidad de objetos administrados	209
Compatibilidad de herramientas de administración	210
Compatibilidad de clientes	210
Actualización de la Versión 2 de Message Queue	210
Tareas previas a la actualización	211
Actualización de la Versión 2 de Message Queue (Solaris)	212
Actualización de la Versión 2 de Message Queue (Linux)	214
Instalación del paquete de compatibilidad (Linux)	216
Verificación de la actualización de Message Queue	216
Tareas posteriores a la actualización	216
Anulación de la actualización	217
Actualización de varias instancias	217
 Capítulo11 Application Server	 219
Visión general de la actualización de Application Server	221
Acerca de Application Server de Java ES Versión 5	221
Guía de actualización de Application Server	221
Datos de Application Server	224
Estrategia de actualización para Application Server	225
Problemas de compatibilidad	225

Dependencias de Application Server	225
Actualización de Application Server desde Java ES Versión 4	227
Introducción	227
Actualización de la Versión 4 de Application Server	228
Tareas previas a la actualización	228
Actualización de la Versión 4 de Application Server	230
Verificación de la actualización	232
Tareas posteriores a la actualización	232
Anulación de la actualización	233
Actualización de Application Server desde Java ES Versión 3	234
Actualización de Application Server desde Java ES Versión 2	235
Introducción	235
Actualización de la Versión 2 de Application Server	236
Tareas previas a la actualización	236
Actualización de la Versión 2 de Application Server (Solaris)	239
Actualización de la Versión 2 de Application Server (Linux)	244
Verificación de la actualización	244
Tareas posteriores a la actualización	244
Anulación de la actualización	245
Actualización de Application Server integrado en Solaris en un entorno de zonas múltiples de Solaris	
10	246
 Capítulo12 Service Registry	249
Visión general de las actualizaciones de Service Registry	251
Acerca de Java ES Versión 5	251
Guía de actualización de Java ES Versión 5	251
Datos de Service Registry	252
Estrategia de actualización para Service Registry	252
Problemas de compatibilidad	252
Dependencias	253
Actualización de Service Registry desde Java ES Versión 4	254
Introducción	254
Actualización de la Versión 4 de Service Registry	255
Tareas previas a la actualización	255
Actualización de la Versión 4 de Service Registry	257
Verificación de la actualización	260
Tareas posteriores a la actualización	261
Anulación de la actualización	261
Actualización de varias instancias	262
 Capítulo13 Web Proxy Server	263
Visión general de la actualización de Web Proxy Server	264

Acerca de Web Proxy Server de Java ES Versión 5	264
Guía de actualización de Web Proxy Server	264
Datos de Web Proxy Server	265
Estrategia de actualización para Web Proxy Server	265
Problemas de compatibilidad	266
Web Proxy ServerDependencias	266
Actualización de Web Proxy Server desde Java ES Versión 4	267
Introducción	267
Actualización de la Versión 4 de Web Proxy Server	268
Tareas previas a la actualización	268
Actualización de la Versión 4 de Web Proxy Server (Solaris)	269
Actualización de la Versión 4 de Web Proxy Server (Linux)	271
Verificación de la actualización	272
Tareas posteriores a la actualización	272
Deshacer la actualización (Solaris)	273
Actualización de Web Proxy Server desde la Versión 3.6	274
Introducción	274
Actualización de la Versión 3.6 de Web Proxy Server	275
Tareas previas a la actualización	275
Actualización de la Versión 3.6 Web Proxy Server	276
Verificación de la actualización	278
Tareas posteriores a la actualización	278
Anulación de la actualización de la Versión 3.6	279
 Capítulo14 Access Manager	281
Visión general de la actualización de Access Manager	282
Acerca de Access Manager de Java ES Versión 5	282
Guía de actualización de Access Manager	283
Datos de Access Manager	285
Estrategia de actualización para Access Manager	286
Problemas de compatibilidad	286
Dependencias de Access Manager	287
Escenarios de actualización del contenedor web	288
Actualización de Access Manager desde Java ES Versión 4	290
Introducción	290
Actualización completa de la Versión 4 de Access Manager	291
Tareas previas a la actualización	291
Actualización de la Versión 4 de Access Manager	295
Verificación de la actualización de Access Manager	306
Tareas posteriores a la actualización	307
Anulación de la actualización	308
Actualización de varias instancias	309
Actualización sólo de Access Manager SDK de la Versión 4	311

Tareas previas a la actualización	312
Actualización del componente de Access Manager SDK de la Versión 4	312
Verificación de la actualización de Access Manager SDK	313
Anulación de la actualización	314
Actualización de Access Manager desde Java ES Versión 3	315
Actualización de la Versión 3 de Access Manager	315
Actualización de varias instancias	315
Actualización de Access Manager desde Java ES Versión 2	320
Tareas previas a la actualización	320
Actualización de las dependencias de Access Manager	321
Actualice el esquema de directorio	321
Vuelva a indexar el directorio	321
Actualización de la Versión 2 de Access Manager	323
Actualización de la Versión 2 de Access Manager: contenedor web Web Server	323
Actualización de la Versión 2 de Access Manager: contenedor web Application Server	323
Verificación de la actualización de Access Manager	334
Tareas posteriores a la actualización	334
Anulación de la actualización	335
Actualización de varias instancias	335
 Capítulo15 Portal Server	337
Visión general de la actualización de Portal Server	339
Acerca de Portal Server de Java ES Versión 5	339
Guía de actualización de Portal Server	339
Datos de Portal Server	340
Estrategia de actualización para Portal Server	341
Problemas de compatibilidad	342
Portal ServerDependencias	342
Problemas de la actualización selectiva	343
Escenarios de actualización del contenedor web	344
Actualización de Portal Server desde Java ES Versión 4	346
Introducción	346
Actualización de la Versión 4 de Portal Server	348
Tareas previas a la actualización de la Versión 4	349
Actualización de la Versión 4 de Portal Server (Solaris)	355
Actualización de la Versión 4 de Portal Server (Linux)	359
Verificación de la actualización	362
Tareas posteriores a la actualización de la Versión 4	363
Deshacer la actualización (Solaris)	370
Anulación de la actualización (Linux)	372
Actualización de varias instancias	372
Actualización de Portal Server desde Java ES Versión 3	377

Tarea previa a la actualización de la Versión 3: actualización de las dependencias de Portal Server	377
Actualización de la Versión 3 de Portal Server	378
Tareas posteriores a la actualización de la Versión 3	378
Suscripción a un debate	378
Actualización de varias instancias	379
Actualización de Portal Server desde Java ES Versión 2	380
Tareas previas a la actualización de la Versión 2	380
Actualización de la Versión 2 de Portal Server	381
Actualización de la Versión 2 de Portal Server: contenedor web Web Server	381
Actualización de la Versión 2 de Portal Server: contenedor web Application Server	382
Tareas posteriores a la actualización de la Versión 2	386
Configuración del inicio de sesión único	386
Habilite el canal URLScrapper	390
Elimine la entrada del servicio de la puerta de enlace	390
Actualización de varias instancias	390
Actualización de Portal Server desde la Versión intermedia 7.0	391
Introducción a la actualización de la versión Portal Server IFR	391
Actualización de Portal Server IFR 7.0	392
Tareas previas a la actualización de IFR 7	393
Actualización de Portal Server IFR 7.0 (Solaris)	393
Actualización de la versión IFR 7 de Portal Server (Linux)	396
Procedimiento de actualización de IFR 7 (Linux)	396
Verificación de la actualización	399
Tareas posteriores a la actualización de IFR 7	400
Deshacer la actualización (Solaris)	407
Anulación de la actualización (Linux)	409
Actualización de varias instancias	409
Capítulo16 Portal Server Secure Remote Access	411
Visión general de la actualización de Portal Server Secure Remote Access	413
Acerca de Portal Server Secure Remote Access de Java ES Versión 5	413
Guía de actualización de Portal Server Secure Remote Access	413
Datos de Portal Server Secure Remote Access	414
Estrategia de actualización para Portal Server Secure Remote Access	415
Problemas de compatibilidad	415
Portal Server Secure Remote AccessDependencias	416
Problemas de la actualización selectiva	417
Actualización de Portal Server Secure Remote Access desde Java ES Versión 4	418
Introducción	418
Actualización de la Versión 4 de Portal Server Secure Remote Access	420
Tareas previas a la actualización de la Versión 4	420
Actualización de la Versión 4 de Portal Server Secure Remote Access (Solaris)	424

Actualización de la Versión 4 de Portal Server Secure Remote Access (Linux)	427
Verificación de la actualización	429
Tareas posteriores a la actualización de la Versión 4	429
Deshacer la actualización (Solaris)	431
Anulación de la actualización (Linux)	433
Actualización de varias instancias	433
Actualización de Portal Server Secure Remote Access desde Java ES Versión 3	439
Actualización de las dependencias de Portal Server Secure Remote Access	439
Actualización de la Versión 3 de Portal Server Secure Remote Access	440
Actualización de varias instancias	440
Actualización de Portal Server Secure Remote Access desde Java ES Versión 2	441
Tareas previas a la actualización de la Versión 2	441
Actualización de las dependencias de Portal Server Secure Remote Access	441
Elimine la entrada del servicio de la puerta de enlace	442
Actualización de la Versión 2 de Portal Server Secure Remote Access	442
Tareas posteriores a la actualización de la Versión 2	443
Establezca el dominio de Portal Server para el servicio Proxylet	443
Actualización de varias instancias	443
Actualización de Portal Server Secure Remote Access desde la Versión intermedia 7.0	444
Introducción	444
Actualización de Portal Server Secure Remote Access IFR 7.0	445
Tareas previas a la actualización	445
Actualización de Portal Server Secure Remote Access IFR 7.0 (Solaris)	445
Actualización de Portal Server Secure Remote Access IFR 7.0 (Linux)	447
Procedimiento de actualización de IFR 7 (Linux)	447
Verificación de la actualización	449
Tareas posteriores a la actualización	450
Deshacer la actualización (Solaris)	450
Anulación de la actualización (Linux)	450
Actualización de varias instancias	451
 Apéndice A Contenido de las versiones de Java Enterprise System	453
Java ES 2003Q4 (Versión 1)	454
Componentes de la Versión 1 que se pueden seleccionar en el programa de instalación	454
Componentes compartidos de la Versión 1	455
Java ES 2004Q2 (Versión 2)	456
Componentes de la Versión 2 que se pueden seleccionar en el programa de instalación	456
Componentes compartidos de la Versión 2	457
Java ES 2005Q1 (Versión 3)	459
Componentes de la Versión 3 que se pueden seleccionar en el programa de instalación	459
Componentes compartidos de la Versión 3	462
Java ES 2005Q4 (Versión 4)	464
Componentes de la Versión 4 que se pueden seleccionar en el programa de instalación	464

Componentes compartidos de la Versión 4	467
Java ES 5 (Versión 5)	469
Componentes de la Versión 5 que se pueden seleccionar en el programa de instalación	469
Componentes compartidos de la Versión 5	472
Índice	475

Lista de tablas

Tabla 1	Convenciones tipográficas	23
Tabla 2	Convenciones de símbolos	23
Tabla 3	Indicadores de intérprete de comandos	24
Tabla 4	Java Enterprise System Documentación	25
Tabla 1-1	Java ES 5 Product Components	30
Tabla 1-2	Java ES Componentes compartidos de Java ES 5	31
Tabla 1-3	Enfoques de actualización de los componentes de productos de Java ES	36
Tabla 1-4	Fases del proceso de actualización	39
Tabla 1-5	Rutas de actualización a Java ES 5 (Versión 5)	42
Tabla 1-6	Actualización selectiva en comparación con la Actualización completa	45
Tabla 1-7	Dependencias de los componentes de productos de Java ES 5 (Versión 5) con los componentes compartidos	49
Tabla 1-8	Dependencias entre los componentes de productos de Java ES	53
Tabla 1-9	Revisiones necesarias cuando no se actualiza Application Server a la Versión 5 ...	61
Tabla 2-1	Enlace simbólico a JAVE SE según la plataforma	76
Tabla 2-2	Resultados de la verificación de la versión de Java SE	77
Tabla 2-3	Rutas de directorio del contenedor de agentes común	78
Tabla 3-1	Rutas de actualización a Java ES 5 (Versión 5): Software de Sun Cluster 3.1 8/05 ...	83
Tabla 3-2	Uso de datos de Sun Cluster	84
Tabla 3-3	Sun Cluster Resultados de la verificación de la versión	89
Tabla 4-1	Sun Cluster Geographic Edition Rutas de directorio	95
Tabla 4-2	Rutas de actualización a Java ES 5 (Versión 5): Sun Cluster Geographic Edition 3.1 2006Q4	96
Tabla 4-3	Uso de datos de Sun Cluster Geographic Edition	97
Tabla 4-4	Resultados de la verificación de la versión de Sun Cluster Geographic Edition	100

Tabla 5-1	Directory Server Rutas de directorio	108
Tabla 5-2	Rutas de actualización a Java ES 5 (Versión 5): Directory Server 6.0	109
Tabla 5-3	Uso de datos de Directory Server	111
Tabla 5-4	Resultados de la verificación de la versión de Directory Server	115
Tabla 6-1	Directory Proxy Server Rutas de directorio	126
Tabla 6-2	Rutas de actualización a Java ES 5 (Versión 5): Directory Proxy Server 6.0	128
Tabla 6-3	Uso de datos de Directory Proxy Server	129
Tabla 6-4	Resultados de la verificación de la versión de Directory Proxy Server	133
Tabla 7-1	Web Server Rutas de directorio	141
Tabla 7-2	Rutas de actualización a Java ES 5 (Versión 5): Web Server 7.0	143
Tabla 7-3	Uso de datos de Web Server	144
Tabla 7-4	Nombres predeterminados de Web Server	145
Tabla 7-5	Resultados de la verificación de la versión de Web Server	147
Tabla 7-6	Valores de <code>WSInstall.properties</code>	153
Tabla 7-7	Opciones de comandos comunes de <code>wadm</code>	156
Tabla 7-8	Opciones y operandos del comando <code>wadm migrate-server</code>	158
Tabla 7-9	Opciones y operandos del comando <code>wadm create-instance</code>	161
Tabla 7-10	Opciones y operandos del comando <code>wadm deploy-cofig</code>	161
Tabla 7-11	Opciones y operandos del comando <code>wadm set-virtual-server-prop</code>	163
Tabla 7-12	Opciones y operandos del comando <code>wadm set-search-collection-prop</code>	165
Tabla 8-1	Java DB Rutas de directorio	171
Tabla 8-2	Rutas de actualización a Java ES 5 (Versión 5): Java DB 10.1.3	172
Tabla 8-3	Uso de datos de Java DB	173
Tabla 8-4	Resultados de la verificación de la versión de Java DB	175
Tabla 9-1	HADB Rutas de directorio	180
Tabla 9-2	Rutas de actualización a Java ES 5 (Versión 5): HADB 4.4.3	181
Tabla 9-3	Uso de datos de HADB	182
Tabla 9-4	Resultados de la verificación de la versión de HADB	185
Tabla 9-5	Versiones de los paquetes de actualización de HADB en las plataformas Solaris ..	187
Tabla 10-1	Message Queue Rutas de directorio	193
Tabla 10-2	Rutas de actualización a Java ES 5 (Versión 5): Message Queue 3.7 UR1	195
Tabla 10-3	Message Queue Uso de datos (SO Solaris)	196
Tabla 10-4	Resultados de la verificación de la versión de Message Queue	201
Tabla 10-5	Resultados de la verificación de la versión de Message Queue	211

Tabla 11-1	Application Server Rutas de directorio	220
Tabla 11-2	Rutas de actualización a Java ES 5 (Versión 5): Application Server Enterprise Edition 8.2	222
Tabla 11-3	Rutas de actualización para las versiones integradas de Application Server con el sistema operativo Solaris	223
Tabla 11-4	Uso de datos de Application Server	224
Tabla 11-5	Resultados de la verificación de la versión de Application Server	229
Tabla 12-1	Service Registry Rutas de directorio	249
Tabla 12-2	Rutas de actualización a Java ES 5 (Versión 5): Service Registry 3.1	251
Tabla 12-3	Uso de datos de Service Registry	252
Tabla 12-4	Resultados de la verificación de la versión de Service Registry	256
Tabla 13-1	Web Proxy Server Rutas de directorio	263
Tabla 13-2	Rutas de actualización a Java ES 5 (Versión 5): Web Proxy Server 4.0.4	264
Tabla 13-3	Uso de datos de Web Proxy Server	265
Tabla 13-4	Web Proxy Server Resultados de la verificación de la versión	268
Tabla 13-5	Revisiones de actualización de Web Proxy Server en Solaris	269
Tabla 13-6	Revisiones de actualización de Web Proxy Server en Linux	271
Tabla 13-7	Resultados de la verificación de la versión de Web Proxy Server	275
Tabla 14-1	Access Manager Rutas de directorio	282
Tabla 14-2	Rutas de actualización a Java ES 5 (Versión 5): Access Manager 7.1	283
Tabla 14-3	Uso de datos de Access Manager	285
Tabla 14-4	Escenarios de actualización del contenedor web para la actualización de Access Manager	288
Tabla 14-5	Resultados de la verificación de la versión de Access Manager	292
Tabla 14-6	Revisiones de actualización del software de acceso móvil de Access Manager	296
Tabla 14-7	Parámetros de revisión de Mobile Access	297
Tabla 14-8	Parámetros de configuración de Access Manager ampre71upgrade	297
Tabla 14-9	Modos de Administrative Server admitidos por amconfig	301
Tabla 14-10	Parámetros de configuración de Access Manager amconfig	302
Tabla 14-11	Parámetros de amconfig: Versión 5Web Server	304
Tabla 14-12	Parámetros de configuración de Access Manager amupgrade	305
Tabla 14-13	Revisiones para la actualización del software de acceso móvil de Access Manager	325
Tabla 14-14	Parámetros de revisión de Mobile Access	325
Tabla 14-15	Parámetros de configuración de Access Manager ampre71upgrade	326
Tabla 14-16	Parámetros de configuración de Access Manager amconfig	330

Tabla 14-17	Parámetros de configuración de Access Manager amupgrade	333
Tabla 15-1	Portal Server Rutas de directorio	338
Tabla 15-2	Rutas de actualización a Java ES 5 (Versión 5): Portal Server 7.1	340
Tabla 15-3	Portal Server Uso de datos	340
Tabla 15-4	Escenarios de actualización del contenedor web para la actualización de Portal Server 344	
Tabla 15-5	Resultados de la verificación de la versión de Portal Server	349
Tabla 15-6	Información necesaria para la secuencia de comandos psupgrade según el escenario de actualización del contenedor web	351
Tabla 15-7	Ubicación de la configuración de JVM	354
Tabla 15-8	Revisiones para actualizar Portal Server IFR a la Versión 5	391
Tabla 16-1	Portal Server Secure Remote Access Rutas de directorio	412
Tabla 16-2	Rutas de actualización a Java ES 5 (Versión 5): Portal Server Secure Remote Access 7.1 414	
Tabla 16-3	Portal Server Secure Remote Access Uso de datos	415
Tabla 16-4	Resultados de la verificación de la versión de Portal Server Secure Remote Access	421
Tabla 16-5	Revisiones para actualizar Portal Server Secure Remote Access IFR a la Versión 5 .	444

Prefacio

La *Java Enterprise System Guía de actualización para UNIX* contiene la información necesaria para actualizar el software de Sun Java™ Enterprise System (Java ES) en el sistema operativo Sun Solaris™ (SO Solaris) o el entorno del sistema operativo Red Hat Enterprise Linux (RHEL). No describe la actualización en un entorno HP-UX.

Esta guía describe la actualización de Java ES 2004Q2 (Versión 2), Java ES 2005Q1 (Versión 3) y Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5).

Este prefacio contiene las siguientes secciones:

- “Público objetivo de este libro” en la página 22
- “Convenciones utilizadas en este libro” en la página 22
- “Documentación relacionada” en la página 24
- “Acceso en línea a recursos de Sun” en la página 27
- “Contacto con el servicio técnico de Sun” en la página 27
- “Referencias a sitios web de terceros” en la página 27
- “Sun valora sus comentarios” en la página 28

Público objetivo de este libro

Esta guía está dirigida a administradores de sistemas o técnicos de software que desean actualizar el software de Java ES.

Este libro asume que está familiarizado con las siguientes operaciones:

- Instalación de productos de software en el ámbito de la empresa
- Los componentes de Java ES implementados actualmente en su entorno
- Administración de sistemas y trabajo en red en la plataforma Java ES compatible
- Modelo de clúster (si está instalando software para clúster)

Convenciones utilizadas en este libro

Las tablas de esta sección describen las convenciones utilizadas en este libro.

Interfaces administrativas

En la mayoría de los procedimientos de actualización descritos en esta *Guía de actualización* se pueden utilizar dos interfaces administrativas: una interfaz gráfica de usuario (GUI) y una interfaz de la línea de comandos.

En la mayoría de los casos, en esta *Guía de actualización* se utiliza la interfaz de la línea de comandos cuando se describen los procedimientos de actualización de componentes de Java ES. La interfaz de la línea de comandos puede utilizarse para crear secuencias de comandos en la actualización de las implementaciones de Java ES, de manera que este procedimiento pueda repetirse fácilmente cuando sea necesario.

Cuando en los procedimientos se utiliza el programa de instalación de Java ES se describe, sin embargo, la interfaz GUI en lugar de la interfaz interactiva basada en texto. Las sesiones del programa de instalación de Java ES pueden guardarse en un archivo de estado que puede utilizarse para repetir los procedimientos cuando sea necesario.

Convenciones tipográficas

La siguiente tabla describe los cambios tipográficos utilizados en este libro.

Tabla 1 Convenciones tipográficas

Tipos de letra	Significado	Ejemplos
AaBbCc123 (un espacio)	API y elementos de idioma, etiquetas HTML, direcciones URL de sitio web, nombres de comandos, nombres de archivos, nombres de rutas de directorios, mensajes en pantalla, código de ejemplo.	Edite el archivo <code>.login</code> . Utilice <code>ls -a</code> para ver una lista de todos los archivos. <code>% Tiene correo.</code>
AaBbCc123 (un espacio en negrita)	Lo que escribe, para resaltarlo con respecto a lo que aparece en pantalla.	% su Contraseña:
<i>AaBbCc123</i> (cursiva)	Títulos de libros, términos nuevos, palabras que se desea destacar. Un marcador en un comando o nombre de ruta que se va a sustituir con un nombre o valor real.	Consulte el capítulo 6 de <i>User's Guide</i> . Éstas se denominan opciones de <i>clase</i> . <i>No</i> guarde el archivo. El archivo se encuentra en el directorio <i>install-dir/bin</i> .

Símbolos

La siguiente tabla describe las convenciones de símbolos utilizadas en este libro.

Tabla 2 Convenciones de símbolos

Símbolo	Descripción	Ejemplo	Significado
[]	Contiene opciones de comandos.	<code>ls [-l]</code>	La opción <code>-l</code> no es obligatoria.
{ }	Contiene un conjunto de opciones para una opción de comando obligatoria.	<code>-d {y n}</code>	La opción <code>-d</code> requiere que se utilice el argumento <code>y</code> o <code>n</code> .
-	Une varias pulsaciones de teclas simultáneas.	Control-A	Pulse la tecla Control a la vez que pulsa la tecla A.

Tabla 2 Convenciones de símbolos (*continúa*)

Símbolo	Descripción	Ejemplo	Significado
+	Une varias pulsaciones de teclas consecutivas.	Ctrl+A+N	Pulse la tecla Control, suéltela y pulse las siguientes teclas.
>	Indica las selecciones de elementos de menú en una interfaz gráfica de usuario.	Archivo > Nuevo > Plantillas	En el menú Archivo, seleccione Nuevo. En el menú secundario Nuevo, elija Plantillas.

Indicadores de intérprete de comandos

La siguiente tabla muestra los indicadores de intérprete de comandos utilizados en esta guía.

Tabla 3 Indicadores de intérprete de comandos

Intérprete de comandos	Indicador
Intérprete de comandos C en UNIX o Linux	<i>nombre-máquina%</i>
Superusuario de intérprete de comandos C en UNIX o Linux	<i>nombre-máquina#</i>
Intérprete de comandos Bourne y Korn en UNIX o Linux	\$
Superusuario de intérprete de comandos Bourne y Korn en UNIX o Linux	#
Línea de comandos de Windows	C:\

Documentación relacionada

El sitio web <http://docs.sun.com>SM permite acceder a la documentación técnica de Sun en línea. Puede buscar el archivo o buscar un título de guía o asunto específico.

Guías incluidas en este conjunto de documentación de Java ES

Los manuales de Java ES se encuentran disponibles como archivos en línea con formato PDF (Formato de documento portátil) y HTML (Lenguaje de marcado de hipertexto). Los dos formatos se pueden leer mediante tecnologías de asistencia para usuarios con discapacidades. Se puede acceder al sitio Web de la documentación de Sun™ en:

<http://docs.sun.com>

La documentación de Java ES incluye información acerca del sistema como una unidad completa y también de sus componentes. Se puede acceder a la documentación en:

<http://docs.sun.com/coll/1286.2>

La siguiente tabla enumera los manuales sobre el sistema incluidos en el conjunto de documentación de Java ES. La columna de la izquierda especifica el nombre y la ubicación del número de referencia de cada documento y la columna de la derecha describe el contenido general del documento.

Tabla 4 Java Enterprise System Documentación

Documento	Contenido
<i>Notas de la versión de Java Enterprise System 5 para UNIX</i> http://docs.sun.com/doc/819-4893	Incluye la información más reciente acerca de Java ES, entre la que se encuentran los problemas conocidos. Además, cada componente tiene sus propias notas de la versión.
<i>Java Enterprise System 5 Technical Overview</i> http://docs.sun.com/doc/820-0167	Presenta los fundamentos conceptuales y técnicos de Java ES. Describe los componentes, la arquitectura, los procesos y las funciones.
<i>Guía de planificación de la implementación de Java Enterprise System</i> http://docs.sun.com/doc/819-2326	Proporciona una introducción a la planificación y el diseño de soluciones de implementación empresarial basadas en Java ES. Presenta los conceptos y principios básicos del diseño y la planificación de la implementación, plantea el ciclo de vida de la solución y proporciona ejemplos y estrategias generales para utilizarlas cuando se planifiquen soluciones basadas en Java ES.

Tabla 4 Java Enterprise System Documentación (*continúa*)

Documento	Contenido
<i>Guía de planificación de la instalación de Java Enterprise System 5</i> http://docs.sun.com/doc/819-5079	Le ayuda a desarrollar las especificaciones de implementación para el hardware, el sistema operativo y los aspectos de red de su implementación de Java ES. Describe algunos aspectos como las dependencias de los componentes, que se deben abordar en la planificación de la instalación y la configuración.
<i>Guía de instalación de Java Enterprise System 5 para UNIX</i> http://docs.sun.com/doc/819-4891	Le guía en el proceso de instalación de Java ES en el sistema operativo Solaris o en el sistema operativo Linux. También muestra cómo configurar los componentes después de la instalación y comprobar que funcionen correctamente.
<i>Referencia de instalación de Java Enterprise System 5 para UNIX</i> http://docs.sun.com/doc/819-4892	Ofrece información adicional sobre los parámetros de configuración, proporciona hojas de cálculo para la planificación de la configuración y muestra el material de referencia como, por ejemplo, los números de puerto y los directorios predeterminados.
<i>Guía de actualización de Java Enterprise System 5 para UNIX</i> http://docs.sun.com/doc/819-6553	Proporciona instrucciones para actualizar Java ES en el sistema operativo Solaris o en el entorno operativo Linux.
<i>Guía de supervisión de Sun Java Enterprise System 5</i> http://docs.sun.com/doc/819-5081	Proporciona instrucciones para establecer la estructura de supervisión de cada componente de producto y utilizar la consola de supervisión para ver los datos en tiempo real y establecer alarmas de umbral.
<i>Java Enterprise System Glossary</i> http://docs.sun.com/doc/819-3875	Define los términos utilizados en la documentación de Java ES.

Cómo buscar documentación sobre productos de Sun

Además de buscar documentación sobre los productos de Sun en el sitio web `docs.sun.com`, puede utilizar un motor de búsqueda, para lo que tendrá que escribir en el campo de búsqueda la siguiente sintaxis:

`search-term sitio:docs.sun.com`

Por ejemplo, si quiere buscar el término “agente”, escriba:

`agente sitio:docs.sun.com`

Si quiere incluir otros sitios de Sun en la búsqueda (por ejemplo, java.sun.com, www.sun.com, developers.sun.com), utilice en el campo de búsqueda sun.com en lugar de docs.sun.com.

Acceso en línea a recursos de Sun

Para obtener descargas de productos, servicios profesionales, revisiones y servicio técnico, así como información adicional para los desarrolladores, acuda a:

- Centro de descargas
<http://www.sun.com/software/download/>
- Soluciones de cliente
<http://www.sun.com/service/sunjavasystem/sjsservicessuite.html>
- Servicios empresariales de Sun, revisiones de Solaris y servicio técnico
<http://sunsolve.sun.com/>
- Información para programadores
<http://developers.sun.com>

La siguiente ubicación contiene información acerca de Java Enterprise System y sus componentes:

<http://www.sun.com/software/javaenterprisesystem/index.html>

Contacto con el servicio técnico de Sun

Si tiene preguntas técnicas acerca de este producto que no se respondan en la documentación de productos, vaya a <http://www.sun.com/service/contacting>.

Referencias a sitios web de terceros

Sun no se hace responsable de la disponibilidad de los sitios web de terceros mencionados en este documento. Sun no respalda ni se hace responsable de ningún contenido, anuncio, producto o cualquier otro material disponible en dichos sitios o recursos. Asimismo, Sun no se responsabiliza de ningún daño, real o supuesto, ni de posibles pérdidas que se pudieran derivar del uso de los contenidos, bienes o servicios que estén disponibles en dichos sitios o recursos.

Sun valora sus comentarios

Sun tiene interés en mejorar su documentación y valora sus comentarios y sugerencias.

Para publicar sus comentarios, acceda a <http://docs.sun.com> y haga clic en “Send Comments” (Enviar comentarios). Se mostrará un formulario en línea en el que deberá indicar el título del documento y el número de referencia. El número de referencia consta de siete o de nueve dígitos, y se encuentra en la página que contiene el título de la guía o al principio del documento.

Planificación de las actualizaciones

En este capítulo se proporciona información para planificar la actualización del software de Sun Java™ Enterprise System (Java ES) a Java ES 5 en el sistema operativo Sun Solaris™ o el entorno de sistema operativo Red Hat Enterprise Linux (denominado simplemente Linux).

Incluye las siguientes secciones:

- “Componentes de Java ES 5” en la página 30
- “Tecnologías de actualización de Java ES” en la página 33
- “El proceso de actualización” en la página 38
- “Consideraciones sobre el plan de actualización” en la página 40
- “Dependencias de los componentes de Java ES” en la página 48
- “Directrices generales de secuenciación” en la página 57
- “Casos especiales” en la página 61
- “Actualización a Java ES 5 y zonas de Solaris 10” en la página 62

Componentes de Java ES 5

En esta sección, que sirve de introducción a la planificación de la actualización del software de Java ES, se revisan los componentes incluidos en Java ES 5 (Versión 5). En función de su escenario de actualización, es posible que necesite actualizar uno o varios de estos componentes a la Versión 5.

Los componentes de Java ES se agrupan en diferentes tipos, tal y como se describe en *Java Enterprise System 5 Technical Overview*, <http://docs.sun.com/doc/819-2330>:

- **Componentes de productos.** Los *componentes de productos* de Java ES están formados por:
 - Componentes de servicios del sistema, que proporcionan los principales servicios de infraestructura de Java ES.
 - Componentes de calidad del servicio, que mejoran los servicios del sistema.

Los componentes de productos se pueden seleccionar en el programa de instalación de Java ES.

- **Componentes compartidos.** Los *componentes compartidos* de Java ES son bibliotecas compartidas de forma local de las que dependen los componentes de productos de Java ES. El programa de instalación de Java ES instala automáticamente los componentes compartidos. Los componentes compartidos que se instalen dependerán de los componentes de productos que se hayan instalado.

Componentes de productos de la Versión 5

Los componentes de productos de la Versión 5 se enumeran en orden alfabético en la siguiente tabla, junto con las abreviaturas utilizadas en las tablas posteriores. Esta tabla incluye el tipo de mejora de servicio que ofrecen los componentes de calidad de servicio.

Tabla 1-1 Java ES 5 Product Components

Componente de producto	Abreviatura	Versión	Tipo
Access Manager	AM	7.1	Componente de servicio del sistema
Application Server	AS	8.2	Componente de servicio del sistema
Directory Proxy Server	DPS	6.0	Calidad de servicio: componente de acceso

Tabla 1-1 Java ES 5 Product Components *(continúa)*

Componente de producto	Abreviatura	Versión	Tipo
Directory Server	DS	6.0	Componente de servicio del sistema
Almacén de sesión de alta disponibilidad	HADB	4.4.3	Calidad de servicio: componente de disponibilidad
Java DB	JavaDB	10.2	Componente de servicio del sistema
Message Queue	MQ	3.7 UR1	Componente de servicio del sistema
Monitoring Console	MC	1.0	Calidad de servicio: componente administrativo
Portal Server	PS	7.1	Componente de servicio del sistema
Portal Server Secure Remote Access	PSRA	7.1	Calidad de servicio: componente de acceso
Service Registry	SR	3.1	Componente de servicio del sistema
Sun Cluster	SC	3.1 8/05	Calidad de servicio: componente de disponibilidad
Sun Cluster Geographic Edition	SCG	2006Q4	Calidad de servicio: componente de disponibilidad
Web Proxy Server	WPS	4.0.4	Calidad de servicio: componente de acceso
Web Server	WS	7.0	Componente de servicio del sistema

Componentes compartidos de la Versión 5

Los componentes compartidos de la Versión 5 se enumeran en orden alfabético en la siguiente tabla, junto con las abreviaturas utilizadas en las tablas posteriores.

Tabla 1-2 Java ES Componentes compartidos de Java ES 5

Componente compartido	Versión	Abreviatura
Apache Commons Logging	1.0.3	ACL
Herramienta de creación basada en Jakarta ANT Java/XML	1.6.5	ANT
Base de datos Berkeley	4.2.52	BDB
Contenedor de agentes común	1.1 y 2.0	CAC
FastInfoSet	1.0.2	FIS

Tabla 1-2 Java ES Componentes compartidos de Java ES 5 (*continúa*)

Componente compartido	Versión	Abreviatura
International Components for Unicode	3.2	ICU
Instant Messenger SDK	6.2.8	IM-SDK
Java Platform, Standard Edition	5.0 Update 7	Java SE
JavaBeans™ Activation Framework	1.0.3	JAF
Java Studio Web Application Framework	2.1.5	JATO
JavaHelp™ runtime	2.0	JHELP
JavaMail™ runtime	1.3.2	JMAIL
Java Architecture for XML Binding runtime	2.0.3	JAXB
Java API for XML Processing	1.3.1	JAXP
Java API for XML Registries runtime	1.0.8	JAXR
Java API for XML-based Remote Procedure Call runtime	1.1.3_01	JAX-RPC
Java API for Web Services runtime	2.0	JAXWS
Java Calendar API	1.2	JCAPI
Java Dynamic Management™ Kit runtime	5.1.2	JDMK
Java Security Services (Servicios de seguridad de redes para Java)	4.2.4 y 3.1.11	JSS y JSS3
JavaServer Pages™ Standard Tag Library	1.0.6	JSTL
KT Search Engine	1.3.4	KTSE
LDAP C SDK	6.0	LDAP C SDK
LDAP Java SDK	4.19	LDAP J SDK
Mobile Access Core	6.2	MA Core
Netscape Portable Runtime	4.6.4	NSPR
Servicios de seguridad de redes	3.11.4	NSS
SOAP Runtime with Attachments API for Java	1.3	SAAJ
Capa de seguridad y autenticación sencilla	2.19	SASL
Sun Explorer Data Collector (sólo para Solaris)	4.3.1	SEDC
Sun Java Monitoring Framework	2.0	MFWK
Sun Java Web Console	3.0.2	SJWC
Web Services Common Library	2.0	WSCL
Seguridad de los servicios web XML	2.0	XWSS

Tecnologías de actualización de Java ES

Ninguna utilidad del sistema actualiza todos los componentes de Java ES. Además, las actualizaciones de los componentes de productos y los componentes compartidos presentan tecnologías y características diferentes, como se describe en las siguientes secciones.

Actualización de componentes de productos

La actualización de los componentes de productos de Java ES a la Versión 5 se realiza componente a componente y equipo a equipo mediante procedimientos de actualización específicos de cada componente, como se describe en esta *Guía de actualización*.

La actualización de los componentes de productos puede variar de una actualización funcional importante, en la que es posible que no haya compatibilidad con la versión anterior del componente, a una actualización para solucionar errores, totalmente compatible con la versión anterior. Debido a las dependencias entre los componentes de Java ES, la naturaleza de una actualización puede influir en la necesidad de actualizar también o no el resto de componentes.

El proceso de actualización de los componentes de productos de Java ES incluye dos operaciones básicas que se asemejan a la instalación y configuración iniciales de los componentes de Java ES:

- **Instalación de las actualizaciones de software.** El software actualizado mejora, arregla o sustituye el software existente. La instalación del software se puede realizar mediante la aplicación de revisiones en los paquetes de software existentes, la sustitución selectiva de los paquetes existentes, la instalación de nuevos paquetes o una nueva instalación completa del software del componente.
- **Reconfiguración** La reconfiguración abarca todos los cambios realizados en los datos de configuración, datos de usuario o datos de aplicación dinámicos necesarios para poder utilizar el software actualizado. Un cambio en los datos puede implicar la inclusión de datos adicionales, un cambio en el formato de los datos (en los archivos de propiedades o en el esquema de base de datos) o una migración de los datos a una nueva ubicación. A veces es necesario llevar a cabo un procedimiento para realizar la reconfiguración y otras veces este proceso se realiza automáticamente. En algunos casos, al realizar la reconfiguración, es necesario también que se vuelva a implementar el software del componente en un contenedor web.

Además, la actualización de los componentes de productos de Java ES conlleva normalmente una serie de tareas previas a la actualización y, en algunos casos, determinados procedimientos posteriores a la actualización que deben realizarse antes de que esté operativa la actualización.

Enfoques de actualización de los componentes de productos

Entre los procedimientos de actualización específicos de los componentes que se utilizan para instalar el software actualizado y realizar la reconfiguración de los componentes, se incluyen los siguientes enfoques de actualización:

- [Uso de la función de actualización del programa de instalación de Java ES](#)
- [Realización de una nueva instalación del componente de producto](#)
- [Ejecución de una utilidad de actualización específica del componente](#)
- [Aplicación de revisiones en los paquetes de componentes existentes](#)

Uso de la función de actualización del programa de instalación de Java ES

El programa de instalación de la Versión 5 incluye una función de actualización que efectúa la actualización de los componentes en determinados casos especiales: Application Server, Message Queue, HADB y Java DB. Cuando el programa de instalación Java ES detecta las versiones instaladas anteriormente de los componentes de productos, marca estos componentes como “actualizables”.

Antes de actualizar estos componentes, el programa de instalación busca las versiones anteriores y actuales de los componentes compartidos. Si el programa de instalación detecta que falta un componente compartido necesario para el componente seleccionado o que presenta una versión anterior, dicho programa actualiza todos los componentes compartidos instalados actualmente e instala los componentes compartidos que faltan y que son necesarios para el componente seleccionado. En algunos casos (sobre todo, en Application Server), el programa de instalación actualizará también los componentes de productos de los que dependa el componente que se está actualizando.

El programa de instalación elimina los paquetes de las versiones anteriores, instala los paquetes de componentes de productos de la Versión 5 y, si es necesario, reconfigura el componente de producto que se está actualizando. (Sin embargo, en el caso de la instancia de Application Server incluida en el sistema operativo Solaris 9, el programa de instalación no elimina los paquetes; consulte [“Actualización de la Versión 2 de Application Server”](#) en la página 236).

Si utiliza la función de zonas del sistema operativo Solaris 10, debe tener en cuenta varias consideraciones especiales. Consulte el [“Compatibilidad con las zonas en el programa de instalación de Java ES”](#) en la página 62.

Realización de una nueva instalación del componente de producto

Algunos componentes de productos se actualizan mediante una nueva instalación de los componentes con el programa de instalación de Java ES. En primer lugar, se eliminan los paquetes de la versión anterior y se instala la Versión 5 en la misma ruta o se instala la Versión 5 en una ruta paralela y se deja la versión anterior intacta.

En ambos casos, debe reconfigurar los componentes de productos. Para ello, debe migrar los datos de configuración de la versión anterior a la nueva instalación, realizar una nueva configuración o realizar una combinación de ambas tareas. Para algunos componentes de productos, se proporciona una utilidad que permite reconfigurar o migrar los datos de configuración de ese componente.

Ejecución de una utilidad de actualización específica del componente

Algunos componentes de productos proporcionan una utilidad o secuencia de comandos de actualización para automatizar la actualización de los componentes a la Versión 5. Esta utilidad realiza normalmente la actualización de los paquetes de software y las tareas de reconfiguración necesarias como parte del proceso de actualización. Para aquellos componentes que se implementen en un contenedor web, la utilidad vuelve a implementar normalmente el software del componente actualizado en el contenedor web.

Aplicación de revisiones en los paquetes de componentes existentes

Para algunos componentes de productos, la actualización se realiza mediante la aplicación manual de revisiones en los paquetes de software existentes. Aunque las plataformas Solaris y Linux emplean tecnologías similares para administrar los paquetes de software instalados y realizar un seguimiento de estos paquetes mediante un registro de paquetes, las diferencias entre las tecnologías de aplicación de revisiones de ambas plataformas afectan a los procedimientos de actualización.

- **Plataforma Solaris.** Los paquetes se instalan y eliminan mediante los comandos `pkgadd` y `pkgrm` de Solaris. Una vez instalado, el contenido del paquete puede modificarse mediante las revisiones aplicadas o eliminadas con los comandos `patchadd` y `patchrm`. Las revisiones para los paquetes de Solaris se distribuyen mediante el sitio web de SunSolve en:
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

Las revisiones de Solaris se pueden aplicar en uno o varios paquetes. El comando `patchadd` guarda el paquete al que se va a aplicar la revisión o realiza una copia de seguridad del mismo para facilitar la eliminación de la revisión mediante el comando `patchrm`. Las revisiones se identifican mediante un Id. de revisión, compuesto por el número de revisión seguido del número de versión que se incrementa a medida que se modifica la revisión con el paso del tiempo.

- **Plataforma Linux.** Los paquetes de Red Hat Enterprise Linux (RPM) se pueden instalar o actualizar mediante el comando rpm. Sin embargo, el contenido del paquete, una vez instalado, no puede modificarse mediante revisiones. En su lugar, los paquetes de RPM se actualizan mediante la opción de comando rpm -U, que sustituye el paquete actual por uno nuevo.

Para mayor comodidad, muchas de las actualizaciones de los paquetes de RPM no sólo se incluyen en la distribución de Java ES Versión 5, sino también mediante el sitio web de SunSolve:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

Para su distribución mediante SunSolve, los paquetes de RPM se encapsulan en revisiones y se les asigna un Id. de revisión y un número de revisión similares a los de las revisiones de Solaris. Estas revisiones de Linux pueden incluir uno o varios paquetes de RPM, cada uno identificado por un nombre de RPM exclusivo, un número de RPM y un número de revisión que aumenta a medida que se modifica el paquete de RPM con el paso del tiempo.

Enfoque de actualización utilizado para cada componente de producto

El enfoque de actualización utilizado para actualizar cada componente de producto a la Versión 5 se muestra en la siguiente tabla:

Tabla 1-3 Enfoques de actualización de los componentes de productos de Java ES

Componente de producto	Instalación del software actualizado	Reconfiguración
Access Manager	Sustituya los paquetes: use una secuencia de comandos de eliminación de paquetes y realice una nueva instalación.	Use las secuencias de comandos amconfig y amupgrade para la reconfiguración y la nueva implementación en el contenedor web.
Application Server	Sustituya los paquetes: use la función de actualización del programa de instalación de Java ES.	Ninguna, excepto en la actualización desde la Versión 2; use las secuencias de comandos postinstall y asupgrade.
Directory Proxy Server	Realice una nueva instalación sin sustituir los paquetes anteriores.	Reconfiguración manual
Directory Server	Realice una nueva instalación sin sustituir los paquetes anteriores.	Use el comando dsmig para migrar los datos del directorio.

Tabla 1-3 Enfoques de actualización de los componentes de productos de Java ES

Componente de producto	Instalación del software actualizado	Reconfiguración
Almacén de sesión de alta disponibilidad	Sustituya los paquetes: use la función de actualización de Java ES o realice una nueva instalación paralela.	Ninguna
Java DB	Sustituya los paquetes: use la función de actualización del programa de instalación de Java ES.	Ninguna
Message Queue	Sustituya los paquetes: use la función de actualización del programa de instalación de Java ES o la secuencia de comandos mqupgrade (desde la Versión 2).	Ninguna, excepto en la actualización desde la Versión 2 en Linux; use la secuencia de comandos mqmigrate.
Portal Server	Sustituya los paquetes: use la secuencia de comandos psupgrade.	Use la secuencia de comandos psupgrade para la reconfiguración y la nueva implementación en el contenedor web.
Portal Server Secure Remote Access	Sustituya los paquetes: use la secuencia de comandos psupgrade.	Use la secuencia de comandos psupgrade para la reconfiguración.
Service Registry	Realice una nueva instalación sin sustituir los paquetes anteriores.	Realice manualmente la reconfiguración y use la secuencia de comandos ant upgrade para la nueva implementación en el dominio de Application Server.
Sun Cluster	Sustituya los paquetes: use la secuencia de comandos scinstall para sustituir los archivos binarios.	Use la secuencia de comandos scinstall para migrar la configuración.
Sun Cluster Geo	Sustituya los paquetes: use la secuencia de comandos uninstall y realice una nueva instalación.	Ninguna
Web Proxy Server	Aplique las revisiones en los archivos binarios.	Ninguna
Web Server	Realice una nueva instalación sin sustituir los paquetes anteriores.	Use el comando wadm migrate-server para migrar la configuración de la instancia del servidor.

Actualización de los componentes compartidos

La actualización de los componentes compartidos de Java ES es una parte necesaria del proceso de actualización de los componentes de productos que dependen de ellos.

Para actualizar los componentes compartidos, no es necesario realizar la reconfiguración de los componentes ni procedimientos previos o posteriores a la actualización. Además, las actualizaciones de los componentes compartidos no se pueden anular y restablecer a sus versiones anteriores.

El gran número (aprox. 30) de componentes compartidos de Java ES y las complejas interacciones entre éstos y los componentes de productos requieren que se sincronicen todos los componentes compartidos de una única instancia del sistema operativo en la misma versión de Java ES. Una instancia del sistema operativo hace referencia a un único equipo que ejecuta el sistema operativo Solaris 9, Solaris 10 o Red Hat Enterprise Linux, o a cualquier entorno (zona) virtual del sistema operativo en un equipo que ejecute Solaris 10.

Debido al requisito de sincronización, no se deben actualizar individualmente los componentes compartidos de Java ES, sino que deben actualizarse todos simultáneamente a la Versión 5.

La sincronización de los componentes compartidos a la Versión 5 se realiza con el programa de instalación de Java ES. El programa de instalación sincroniza los componentes compartidos al realizar una actualización o una nueva instalación de los componentes de productos (consulte [“Uso de la función de actualización del programa de instalación de Java ES” en la página 34](#)). El programa de instalación incluye también una función de sincronización que actualiza los componentes compartidos existentes e instala los componentes compartidos que falten. Para obtener una descripción más completa de esta función, consulte [“Sincronización de todos los componentes compartidos” en la página 72](#).

El proceso de actualización

El proceso de actualización de Java ES conlleva una serie de fases, que se realizan primero normalmente en el entorno de planificación antes de ejecutarse en un entorno de producción. El uso de un entorno de planificación permite probar cada una de las fases, así como escribir las secuencias de comandos que utilizará el personal de TI para actualizar implementaciones complejas de Java ES.

Una vez que haya probado el proceso de actualización en un entorno de planificación y esté seguro de que funciona correctamente, puede reproducir el proceso en su entorno de producción.

Este proceso conlleva las fases mostradas en la siguiente tabla y descritas en esta *Guía de actualización*. Las fases hacen referencia a las actualizaciones de componentes individuales, así como a la implementación completa de Java ES.

Tabla 1-4 Fases del proceso de actualización

Fase de la actualización	Descripción
Planificación	Debe desarrollar un plan de actualización. En él, debe especificar los componentes de Java ES que se van a actualizar y la secuencia en la que deben actualizar esos componentes en los diferentes equipos o instancias del sistema operativo de su implementación.
Preparación previa a la actualización	Debe realizar una copia de seguridad de los datos de la aplicación y la configuración, aplicar las revisiones del sistema operativo pertinentes, actualizar las dependencias necesarias y realizar otras tareas como preparación para la actualización de un componente individual.
Actualización	Debe obtener todos los paquetes, las revisiones y las herramientas necesarios para la actualización. Debe instalar el software actualizado y reconfigurar cada componente en la forma recomendada, incluida la migración de los datos al sistema actualizado.
Verificación	Debe verificar que la actualización se haya realizado satisfactoriamente mediante las pruebas de verificación recomendadas. Entre estas tareas, se incluyen el inicio de los componentes de software actualizado y la realización de pruebas en los diversos escenarios de uso.
Procedimientos posteriores a la actualización	Debe realizar las tareas adicionales de configuración, personalización o de otro tipo necesarias para que, por ejemplo, el componente actualizado operativo incorpore nuevas funciones.
Anulación/restablecimiento	Anule la actualización y verifique que el proceso de anulación se haya realizado satisfactoriamente. Es importante probar la anulación de la actualización en caso de que, por algún motivo, deba restablecer el entorno de producción a su estado anterior.

Consideraciones sobre el plan de actualización

En un plan de actualización, debe especificar los componentes de Java ES que se van a actualizar a la Versión 5 y la secuencia en la que se actualizarán esos componentes en los diferentes equipos o instancias del sistema operativo de la implementación de Java ES.

Su plan dependerá de sus objetivos y de sus prioridades de actualización, así como del alcance y la complejidad de la arquitectura de implementación.

Por ejemplo, si su arquitectura de implementación de Java ES está formada por un único componente de Java ES que se ejecuta en un único equipo, su objetivo de actualización consistirá en solucionar algunos errores presentes en la versión anterior del software. Por otro lado, si su arquitectura de implementación de Java ES está formada por una serie de componentes interdependientes de Java ES implementados en distintos equipos, su objetivo consistiría en lograr nuevas funciones mediante la actualización del mínimo número de componentes necesarios para alcanzar este fin con el mínimo tiempo de inactividad.

Por lo general, cuanto mayor sea el número de componentes de Java ES, mayor será el número de equipos de la arquitectura de implementación y más complejo será el plan de actualización.

Sin embargo, su plan de actualización dependerá de una serie de consideraciones, además del alcance y la complejidad de su arquitectura de implementación. Estas consideraciones incluyen los siguientes factores:

- [Dependencias de actualización](#)
- [Actualización selectiva o actualización completa](#)
- [Estrategias y rutas de actualización admitidas](#)
- [Actualización de varias instancias](#)
- [Consideraciones sobre el sistema operativo](#)

Dependencias de actualización

Uno de los principales problemas a la hora de planificar la actualización de un componente de producto de Java ES consiste en conocer las dependencias de ese componente con los demás componentes de Java ES y si dichos componentes deben actualizarse para poder realizar la actualización del componente dependiente.

Hay dos tipos de dependencias de actualización:

- **Relación de dependencia de actualización fuerte.** Al actualizar un componente de producto, es necesario actualizar el componente del que depende. Este requisito puede deberse a una nueva función, nuevas interfaces o soluciones de errores necesarias para el componente dependiente. Si existe una relación de dependencia de actualización fuerte, no se puede actualizar ni utilizar satisfactoriamente el componente sin actualizar primero el componente del que depende.
- **Relación de dependencia de actualización leve.** Al actualizar un componente de producto, no es necesario actualizar el componente del que depende. Si existe una relación de dependencia de actualización leve, se puede actualizar y utilizar satisfactoriamente el componente sin actualizar el componente del que depende.

Para actualizar un componente de Java ES, es necesario actualizar todos los componentes con los que tenga *fuertes* relaciones de dependencia, aunque no es obligatorio actualizar los componentes con los que tenga relaciones de dependencia *leves* (con algunas excepciones, como se indica en esta guía). Cuando hay varios componentes interdependientes en un actualización, sólo es necesario actualizar un componente si uno de los componentes de Java ES que se van a actualizar presenta una fuerte relación de dependencia con ese componente específico.

En algunos accesos especiales, debido a las incompatibilidades que se han presentado, al actualizar un componente es necesario actualizar el componente con el que tiene compatibilidad. Estos casos especiales se indican en esta guía.

Estrategias y rutas de actualización admitidas

Su plan de actualización depende de la versión de Java ES que desee actualizar a la Versión 5.

Aunque sea posible actualizar todas las versiones anteriores del software de Java ES a Java ES 5 (Versión 5), las únicas actualizaciones admitidas son las de Java ES 2005Q4 (Versión 4), Java ES 2005Q1 (Versión 3) y Java ES 2004Q2 (Versión 2). Aunque esta *Guía de actualización* proporciona estrategias para realizar actualizaciones desde Java ES 2003Q4 (Versión 1) y las versiones anteriores a Java ES, no se proporcionan los procedimientos para realizar esas actualizaciones.

En la siguiente tabla, se describen las diferentes rutas de actualización a la Versión 5, sus características y las estrategias que se utilizarán al realizar la actualización.

Debido a las diferencias entre las rutas de actualización descritas en la tabla y a que los procedimientos de actualización de los componentes de productos dependen a menudo de la versión que se vaya a actualizar, los capítulos de esta *Guía de actualización* que describen la actualización de los componentes de productos se han dividido en secciones: cada una de ellas representa una ruta de actualización diferente.

Tabla 1-5 Rutas de actualización a Java ES 5 (Versión 5)

Versión del producto	Versión de Java ES	Características del sistema	Estrategias de actualización
2005Q4	Versión 4	Java ES 5 (Versión 5) admite una combinación de componentes de productos de la Versión 4 y la Versión 5 en un único equipo, aunque es necesario que se sincronicen los componentes compartidos a la misma versión. Se ha probado la interoperatividad entre los componentes de productos de la Versión 4 y la Versión 5, y las incompatibilidades detectadas se indican en las <i>Notas de la versión de Java Enterprise System 5 para UNIX</i> , http://docs.sun.com/doc/819-4893 .	La coexistencia entre los componentes de productos de la Versión 4 y la Versión 5 ofrece la posibilidad de actualizar los componentes de productos de la Versión 4 a la Versión 5 de forma selectiva en un único equipo o en una arquitectura de implementación compuesta por varios equipos. Si algún componente de producto de la Versión 5 admite componentes compartidos de la Versión 5, todos los componentes compartidos en el equipo deben sincronizarse a la Versión 5.
2005Q1	Versión 3	Similar a la ruta de actualización de la Versión 4 descrita anteriormente. Java ES 5 (Versión 5) admite una combinación de componentes de productos de la Versión 3 (y también de la Versión 4) y la Versión 5 en un único equipo, aunque es necesario que se sincronicen los componentes compartidos a la misma versión. Se ha probado la interoperatividad entre los componentes de la Versión 3 y la Versión 5, y las incompatibilidades detectadas se indican en las <i>Notas de la versión de Java Enterprise System 5 para UNIX</i> , http://docs.sun.com/doc/819-4893 .	Similar a la ruta de actualización de la Versión 4 descrita anteriormente. La coexistencia entre los componentes de la Versión 3 y la Versión 5 ofrece la posibilidad de actualizar los componentes de la Versión 3 a la Versión 5 de forma selectiva en un único equipo o en una arquitectura de implementación compuesta por varios equipos. Si alguno de los componentes de productos de la Versión 5 necesita la compatibilidad con un componente compartido de la Versión 5, deberán sincronizarse todos los componentes compartidos del equipo a la Versión 5.

Tabla 1-5 Rutas de actualización a Java ES 5 (Versión 5) *(continúa)*

Versión del producto	Versión de Java ES	Características del sistema	Estrategias de actualización
2004Q2	Versión 2	Distinta a las rutas de actualización de la Versión 4 y la Versión 3 descritas anteriormente. Java ES 5 (Versión 5) <i>no</i> admite una combinación de componentes de la Versión 2 y la Versión 5 ni los componentes de productos ni los componentes compartidos en un único equipo. Existen incompatibilidades conocidas entre los componentes de las dos versiones y no se ha verificado (ni se ha probado) la interoperatividad entre los componentes de la Versión 2 y la Versión 5.	Al actualizar los componentes de la Versión 2 a la Versión 5 en un único equipo, deben actualizarse todos los componentes de la Versión 2 a la Versión 5. Sin embargo, a veces es posible combinar componentes de ambas versiones que residan en equipos <i>diferentes</i> en una arquitectura de implementación.
2003Q4 y versiones anteriores	Versión 1 y versiones anteriores a Java ES	Similar a la ruta de actualización de la Versión 2 descrita anteriormente. Java ES 5 (Versión 5) no admite una combinación de componentes de la Versión 2 y la Versión 5 ni los componentes de productos ni los componentes compartidos en un único equipo. Existen incompatibilidades de interfaz conocidas entre los componentes de las dos versiones y no se ha verificado (ni se ha probado) la interoperatividad entre los componentes de la Versión 1 y versiones anteriores, y la Versión 5.	Java ES no certifica la actualización directa de la Versión 1 o anteriores a la Versión 5. Sin embargo, en algunos casos, puede realizar una actualización desde la Versión 1. Para ello, debe actualizar primero a Java ES Versión 3, como se indica en la guía de la Versión 3, <i>Java Enterprise System Upgrade and Migration Guide</i>, http://docs.sun.com/doc/819-0062, y, a continuación, debe actualizar de la Versión 3 a la Versión 5. En dichos casos, se indicará esa posibilidad en el proceso de actualización de ese componente incluido en esta <i>Guía de actualización</i>. En otros casos, se puede realizar la actualización de la Versión 1 a la Versión 5 del mismo modo que la actualización de la Versión 2 o la Versión 3 a la Versión 5. En dichos casos, se indicará esa posibilidad en el proceso de actualización de ese componente incluido en esta <i>Guía de actualización</i>.

NOTA	Cuando se lanza una Versión intermedia (IFR, Interim Feature Release) de los componentes de productos entre las versiones oficiales de Java ES, la actualización de la versión IFR se realiza normalmente mediante el mismo procedimiento que la versión de Java ES anterior. Por ejemplo, si hay una versión IFR entre la Versión 3 y la Versión 4, el componente se actualizaría mediante el procedimiento de actualización de la Versión 3 a la Versión 5. Si éste no es el caso (por ejemplo, para Portal Server y Portal Server Secure Remote Access), esta <i>Guía de actualización</i> describirá el procedimiento específico de la versión IFR.
-------------	---

Actualización selectiva o actualización completa

La distinción entre relaciones de dependencia de actualización fuertes y leves permite actualizar de forma selectiva los componentes de productos de Java ES en un sistema implementado dentro de su plan de actualización. La actualización selectiva se aplica a la actualización de la Versión 3 y la Versión 4 a la Versión 5 en un único equipo. No se permite la actualización selectiva de la Versión 2 a la Versión 5 en un mismo equipo.

Normalmente tiene la opción de realizar una actualización selectiva o completa de los componentes de productos de Java ES en un equipo:

- **Actualización selectiva.** En este enfoque, debe comenzar seleccionando los componentes de productos de Java ES que desee actualizar a la Versión 5. Debe determinar las relaciones de dependencia de actualización fuerte para dicho componente, ya que deberán actualizarse dichos componentes. Repita este proceso para cada relación de dependencia de actualización fuerte hasta que no haya ningún componente más que se deba actualizar. Este ejercicio especifica todos los componentes de productos de Java ES que se deben actualizar.
- **Actualización completa.** En este enfoque, debe actualizar todos los componentes de productos de Java ES a la Versión 5. En algunos casos, debido a la complejidad de una implementación, no es factible por motivos empresariales actualizar todo un sistema a la vez.

La siguiente tabla muestra una comparación de estos dos enfoques de actualización.

Tabla 1-6 Actualización selectiva en comparación con la Actualización completa

Enfoque de actualización	Ventajas	Inconvenientes
Actualización selectiva	Reduce al mínimo el número de componentes que se han de actualizar.	Da como resultado versiones no uniformes para todos los componentes del sistema implementado.
Actualización completa	Mantiene una versión uniforme para todos los componentes del sistema implementado.	Incrementa al máximo el número de componentes que se han de actualizar.

La actualización selectiva se admitía también en Java ES Versión 4. Por lo tanto, pueden coexistir componentes de productos de la Versión 3 y la Versión 4 en un equipo, y ambas versiones se pueden actualizar de forma selectiva a la Versión 5.

Actualización de varias instancias

La secuencia de los procedimientos de actualización de un plan de actualización depende de la forma en que se utilice la redundancia en una arquitectura de implementación. Se pueden utilizar varias instancias de un componente de Java ES para obtener una mayor disponibilidad, escalabilidad, capacidad de servicio o cualquier otra combinación de estas cualidades de servicio. Tres tecnologías utilizan los componentes redundantes en las arquitecturas de implementación de Java ES: el equilibrado de carga (Directory Proxy Server, Web Server, Web Proxy Server, Application Server, Access Manager y Portal Server), las técnicas de alta disponibilidad (Sun Cluster y el Almacén de sesión de alta disponibilidad) y la repetición de Directory Server.

En la mayoría de los casos en los que se utiliza la redundancia, las actualizaciones deben realizarse sin que haya un tiempo de inactividad significativo. Estas actualizaciones por turnos intentan actualizar sucesivamente las instancias redundantes de un componente sin comprometer el servicio que ofrecen.

Las instancias redundantes se suelen implementar en varios equipos. Para la planificación de la actualización, es posible que deba aislar la actualización de los componentes repetidos frente a la actualización de otros componentes para reducir al mínimo el tiempo de inactividad. Debe realizar todas las tareas previas a la actualización para los componentes repetidos en cada equipo antes de realizar la actualización por turnos.

Cada tecnología de repetición incluye procedimientos de configuración o reconfiguración que pueden afectar a la secuencia general de actualización de los componentes de Java ES. Por ejemplo, es posible que sea necesario actualizar Sun Cluster para los componentes que se ejecuten en un entorno de Sun Cluster antes de actualizar los componentes que se estén ejecutando en un entorno de Sun Cluster.

Los capítulos de esta *Guía de actualización* que describen el proceso de actualización de cada componente de producto indican cómo realizar las actualizaciones de varias instancias para sus respectivos componentes.

Consideraciones sobre el sistema operativo

Una serie de consideraciones sobre el sistema operativo pueden afectar a su plan de actualización de Java ES, tal y como se describe a continuación.

Revisiones del sistema operativo necesarias

Para actualizar satisfactoriamente un componente de producto de Java ES, es posible que deba aplicar primero las revisiones del sistema operativo o actualizar el sistema operativo al nivel necesario para el componente de producto de Java ES 5. Sin embargo, en lugar de aplicar las revisiones o soluciones específicas necesarias en cada caso, es preferible establecer todo el sistema en el nivel necesario para Java ES 5 antes de realizar las actualizaciones de los componentes de productos específicos.

- **Plataforma Solaris.** Las revisiones del sistema operativo están disponibles en el sitio web de SunSolve en forma de clúster de revisiones, es decir, un grupo de revisiones del sistema operativo que se pueden aplicar de forma conjunta. Los clústeres de revisiones necesarios para poder utilizar Java ES Versión 5 para Solaris 9 y 10 están disponibles en <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
- **Plataforma Linux.** Las versiones de actualización están disponibles en <https://www.redhat.com/apps/download/>. Sin embargo, no es necesario actualizar previamente el sistema operativo Linux para poder realizar las actualizaciones de Java ES.

Actualizaciones dobles: El software de Java ES y el sistema operativo

Existen dos situaciones que pueden provocar que el sistema operativo y el software de Java ES estén alineados de forma incorrecta, por lo que sería necesario actualizar tanto Java ES como el sistema operativo:

- Se actualiza el sistema operativo a una versión no admitida por el software de Java ES instalado.

Por ejemplo, Java ES 2004Q2 (Versión 2) es compatible con los sistemas operativos Solaris 8 y 9 en Red Hat Enterprise Linux (RHEL) 2.1. Si desea actualizar la plataforma de sistema operativo a Solaris 10 o RHEL 3.0, que no son compatibles con Java ES Versión 2, deberá actualizar también Java ES Versión 2 a una versión de Java ES que sea compatible con la plataforma actualizada, preferiblemente a Java ES 5 (Versión 5).

Puesto que para actualizar algunos componentes de Java ES, es necesario que se estén ejecutando otros componentes de Java ES, no sólo debe actualizar la plataforma de sistema operativo a Solaris 10 o RHEL 3.0 (que no son compatibles con Java ES Versión 2); también debe actualizar a continuación los componentes de Java ES de la Versión 2 a la Versión 5.

- Se actualiza Java ES a una versión no admitida por el software del sistema operativo existente.

Por ejemplo, Java ES 2005Q1 (Versión 3) y Java ES 2005Q4 (Versión 4) se admiten en Solaris 8 y RHEL 2.1. Sin embargo, si desea actualizar Java ES a la Versión 5, que no es compatible con Solaris 8 ni con RHEL 2.1, debe actualizar el sistema operativo a las versiones admitidas por Java ES 5 (Versión 5), preferiblemente a Solaris 10 o RHEL 4.0.

En ambas situaciones, debe actualizar tanto el software de Java ES como el software del sistema operativo. Estas actualizaciones dobles requieren la siguiente secuencia de actualización:

1. Copia de seguridad de las personalizaciones y los archivos de configuración de Java ES.
2. Desinstalación de la versión de Java ES instalada actualmente.
3. Actualización del software del sistema operativo.
4. Realización de una nueva instalación de Java ES 5.
5. Configuración de Java ES 5 con los datos guardados en el [Paso 1](#).

Actualización del sistema operativo

En algunos casos, al actualizar el sistema operativo Solaris, se sobrescriben los componentes compartidos de Java ES existentes por las versiones anteriores. En esos casos, las versiones correctas de Java ES pueden restablecerse mediante la actualización a la Versión 5 de Message Queue, que se incluye en el sistema operativo Solaris. Al actualizar Message Queue, se forzará también la actualización de todos los componentes compartidos que residan en el sistema.

Entornos multizona de Solaris 10

Pueden aparecer una serie de problemas al instalar y actualizar los componentes de Java ES en un entorno multizona. Para obtener una descripción de las ventajas y las limitaciones de la implementación de Java ES en las zonas de Solaris 10 y obtener procedimientos recomendados para la actualización de Java ES en un entorno multizona, consulte [“Actualización a Java ES 5 y zonas de Solaris 10” en la página 62](#).

Dependencias de los componentes de Java ES

Una de las consideraciones más importantes de un plan de actualización es la existencia de relaciones de dependencia entre los diversos componentes de Java ES de un sistema implementado. La secuencia en que se realizan las actualizaciones de los componentes se ve afectada por la naturaleza de las relaciones de dependencia entre ellos.

En esta sección, se proporciona información acerca de las dependencias entre los componentes de Java ES que afectan a su plan de actualización.

- [Dependencias con componentes compartidos](#)
- [Dependencias con componentes de productos](#)

Dependencias con componentes compartidos

La [Tabla 1-7 en la página 49](#) muestra las relaciones de dependencia de los componentes de productos de Java ES 5 (Versión 5) con los componentes compartidos de Java ES. Las abreviaturas de los componentes de productos que aparecen en los encabezados de las columnas de la [Tabla 1-7](#) se han obtenido de la [Tabla 1-1 en la página 30](#). Las abreviaturas de los componentes compartidos aparecen en la [Tabla 1-2 en la página 31](#).

En la matriz de [Tabla 1-7](#) las relaciones fuertes de dependencia para las actualizaciones de la Versión 3 y la Versión 4 a la Versión 5 se marcan con “F”, y las relaciones de dependencia leves se marcan con una “L”. Para las actualizaciones de la Versión 2 a la Versión 5, todas las dependencias de componentes compartidos son, por definición, relaciones de dependencia fuertes; todos los componentes compartidos se deben actualizar de la Versión 2 a la Versión 5.

Tabla 1-7 Dependencias de los componentes de productos de Java ES 5 (Versión 5) con los componentes compartidos

Componente compartido	AM	AS	DPS	DS	Consola de DS	HADB	JavaDB	MQ	PS	PSRA	SC	SCG	SR	WPS	WS
ANT		L							F	F			F		
ACL	L												F		
BDB	L														
CAC	F	L	F	F	F						L ¹	L ¹			
FIS															
ICU		L	F	F					L					L	L
IM-SDK									L						
Java SE	L	L	F	F	F	L	F	L	L	L	L	L	F	L	L
JAF	L	L							L	L			F		
JATO	L	L							L		L	L			
JavaHelp™	L	L						L							L
JavaMail™	L	L							L	L			F		L
JAXB	L	L													L
JAXP	L	L							L	L			F		L
JAXR	L	L											F		L
JAX-RPC	L	L											F		L
JAXWS															L
JCAPI															
JDMK	F	L	F	F	F						L	L			L
JSS	L								L	L				L	L
JSTL															
KTSE									L					L	L
LDAP C SDK	F			F										L	L
LDAP J SDK	L														
MA Core	L								F	F					

Tabla 1-7 Dependencias de los componentes de productos de Java ES 5 (Versión 5) con los componentes compartidos (*continúa*)

Componente compartido	AM	AS	DPS	DS	Consola de DS	HADB	JavaDB	MQ	PS	PSRA	SC	SCG	SR	WPS	WS
MFWK	F			F											
NSPR	L	L	F	F				F	L	L	L	L		L	F
NSS	L	L		F				F	L	L	L	L		L	F
SAAJ	L	L							L	L			F		
SASL				F										L	L
SEDC											L	L			
SJWC	L	L			F						L	L			
WSCL	L	L											F		L
XWSS													F		

1. Ésta es una relación de dependencia específica con la versión 1.1 del contenedor de agentes común (CAC, Common Agent Container).

La [Tabla 1-7](#) de los componentes de productos representa las dependencias directas e indirectas con los componentes compartidos: un componente de producto puede depender de un componente compartido específico (dependencia directa) que, a su vez, dependa de uno o varios componentes compartidos adicionales (dependencia indirecta). La siguiente figura muestra las interdependencias entre los componentes compartidos.

Figura 1-1 Interdependencias entre los componentes compartidos

La [Tabla 1-7](#) muestra los componentes compartidos que deben actualizarse al actualizar uno o varios componentes de productos en un determinado equipo.

Sin embargo, dado que los componentes compartidos se deben sincronizar (consulte [“Actualización de los componentes compartidos” en la página 38](#)), no se pueden actualizar individualmente los componentes compartidos de Java ES, sino que deben actualizarse simultáneamente todos a la Versión 5 en un equipo o en una instancia del sistema operativo.

Si no hay ninguna relación de dependencia de actualización fuerte, no es necesario actualizar los componentes compartidos. Sin embargo, es aconsejable actualizar la base de componentes compartidos de Java ES subyacente a la versión más actual. De hecho, cuando el programa de instalación de Java ES instala o actualiza los componentes de productos, todos los componentes compartidos que residan en el equipo host se sincronizan automáticamente a la Versión 5.

Para obtener información sobre cómo actualizar los componentes compartidos, consulte el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#).

Dependencias con componentes de productos

Las dependencias de los componentes de productos se dividen en dos categorías: dependencias de tiempo de ejecución y dependencias de configuración.

- **Dependencias de tiempo de ejecución.** El funcionamiento de un sistema de software se basa en la interacción entre sus componentes implementados. Las dependencias de infraestructura entre los componentes de producto de Java ES se describen en *Java Enterprise System 5 Technical Overview*. Si un componente de producto de la Versión 5 presenta una fuerte relación de dependencia con otro componente de producto, el componente dependiente sólo se puede actualizar satisfactoriamente y utilizar en la forma prevista si se actualiza también el componente del que depende.
- **Dependencias de configuración.** En algunos casos, se debe instalar, configurar y ejecutar un componente de Java ES para poder configurar otro componente. Por ejemplo, un directorio de usuario/grupo de Directory Server debe estar ejecutándose para poder registrar un servicio de Access Manager. A menudo, en los procedimientos de actualización de componentes, se deben reconfigurar los componentes actualizados o se deben migrar los datos de configuración. Las dependencias de configuración pueden afectar a la secuencia de los procedimientos de actualización.

En las dependencias de tiempo de ejecución, la relación entre los componentes de productos puede ser de tres tipos, como se indica a continuación:

- **Obligatoria.** El componente no puede funcionar sin el componente del que depende.
- **Opcional.** El componente puede funcionar sin el componente del que depende, pero es necesario ese componente para utilizar un subconjunto de sus funciones.
- **Codependencia.** Ambos componentes pueden funcionar sin el apoyo del otro pero, al utilizarlos conjuntamente, pueden proporcionar una mejora en una determinada función o en el rendimiento.

En la siguiente tabla, se muestran las dependencias y las relaciones de dependencia entre los componentes de productos de Java ES mostrados en la [Tabla 1-1 en la página 30](#). Esta información se puede utilizar para determinar las relaciones de dependencia de actualización fuertes que pueden afectar a su plan de actualización.

En la primera columna, se enumeran en orden alfabético los componentes de productos de la Versión 5; en la segunda columna, se muestran otros componentes de Java ES con los que un componente de la Versión 5 presenta una relación de

dependencia; en la tercera columna, se proporcionan las versiones de Java ES que admiten la dependencia de la Versión 5; en la cuarta columna, se describe la relación de dependencia y, en la última columna, se indican las características especiales de la dependencia como, por ejemplo, si el componente del que se depende debe ser local (en contraposición a remoto) o si otros productos de terceros pueden admitir la dependencia.

Si un componente de producto que se va a actualizar a la Versión 5 presenta una relación de dependencia con la Versión 5 de un componente (frente a una versión anterior), el componente del que se depende representa una relación de dependencia de actualización fuerte, por lo que este componente debe actualizarse también a la Versión 5.

Tabla 1-8 Dependencias entre los componentes de productos de Java ES

Componente de producto de la Versión 5	Dependencia ¹	Versión de Java ES	Naturaleza de la dependencia	Características
Access Manager	Directory Server	2-5	Obligatoria: almacena los datos de configuración y permite la búsqueda de datos del usuario.	
	Contenedor web de J2EE:	4-5	Obligatoria: proporciona servicios de tiempo de ejecución de contenedores web.	Sólo local
	- Application Server	4-5		También se admiten:
	- Web Server			- Weblogic ² - WebSphere ³
Access Manager SDK	Access Manager	3-5	Obligatoria: proporciona los servicios de Access Manager.	
Access Manager Autenticación distribuida de Access Manager	Access Manager	4-5	Obligatoria: proporciona los servicios de Access Manager.	
	Contenedor web de J2EE:	4-5	Obligatoria: proporciona servicios de tiempo de ejecución de contenedores web.	Sólo local
	- Application Server	4-5		También se admiten:
	- Web Server			- Weblogic ² - WebSphere ³
Access Manager Conmutación por error de sesión de Access Manager	Access Manager	5	Obligatoria: proporciona los servicios de Access Manager.	
	Message Queue	4-5	Obligatoria: proporciona mensajería asíncrona fiable.	

Tabla 1-8 Dependencias entre los componentes de productos de Java ES *(continúa)*

Componente de producto de la Versión 5	Dependencia ¹	Versión de Java ES	Naturaleza de la dependencia	Características
Application Server	Message Queue	3-5	Obligatoria: proporciona mensajería asíncrona fiable.	Sólo local
	Almacén de sesión de alta disponibilidad (HADB)	5	Obligatoria: almacena el estado de sesión necesario con el fin de permitir la conmutación por error entre las instancias.	Sólo local
	Java DB	5	Obligatoria: proporciona una base de datos predeterminada para los desarrolladores y otro tipo de almacenamiento persistente.	Sólo local
	Web Server	3-5	Opcional: proporciona equilibrado de carga entre las instancias.	Sólo local
Directory Proxy Server	Directory Server	1-5	Codependencia: da como resultado mejoras en la seguridad y en el rendimiento para las solicitudes de directorio. Proporciona datos a Directory Proxy Server.	
Directory Server	Directory Proxy Server	1-5	Codependencia: da como resultado mejoras en la seguridad y en el rendimiento para las solicitudes de directorio. Distribuye la carga y los datos de la caché de Directory Server.	
Almacén de sesión de alta disponibilidad (HADB)	Ninguna			
Java DB	Ninguna			

Tabla 1-8 Dependencias entre los componentes de productos de Java ES (*continúa*)

Componente de producto de la Versión 5	Dependencia ¹	Versión de Java ES	Naturaleza de la dependencia	Características
Message Queue	Directory Server	2-5	Opcional: almacena objetos administrados y datos del usuario.	
	Contenedor web de J2EE:	2-5	Opcional: admite el transporte HTTP entre el cliente y el agente de Message Queue.	
	- Application Server	2-5		
	- Web Server			
	Java DB	5	Opcional: almacena los mensajes persistentes.	Sólo local
Portal Server	Sun Cluster	2-5	Opcional: admite la alta disponibilidad.	
	Directory Server	4-5	Obligatoria: almacena y permite la búsqueda de perfiles del usuario.	
	Contenedor web de J2EE:	4-5	Obligatoria: proporciona servicios de tiempo de ejecución de contenedores web.	Sólo local
	- Application Server	4-5		También se admiten:
	- Web Server			- Weblogic ² - WebSphere ³
	Access Manager Access Manager SDK	4-5	Obligatoria: proporciona servicios de autenticación y autorización, así como inicio de sesión único.	Sólo local (Si la instancia de Access Manager es remota, Access Manager SDK debe utilizarse localmente.)
	Portal Server Secure Remote Access	5	Opcional: proporciona un acceso remoto seguro a través de los componentes de puerta de enlace, proxy Rewriter y proxy Netlet.	
	Cliente de Service Registry	5	Obligatoria: proporciona las bibliotecas necesarias para la compilación	
	Java DB	5	Opcional: proporciona compatibilidad con varias aplicaciones de portlet	

Tabla 1-8 Dependencias entre los componentes de productos de Java ES *(continúa)*

Componente de producto de la Versión 5	Dependencia ¹	Versión de Java ES	Naturaleza de la dependencia	Características
Portal Server Secure Remote Access Puerta de enlace de Portal Server Secure Remote Access	Portal Server	5	Obligatoria: admite la función de puerta de enlace.	
	Access Manager Access Manager SDK	4-5	Obligatoria: proporciona servicios de autenticación y autorización, así como inicio de sesión único.	Sólo local (Si la instancia de Access Manager es remota, Access Manager SDK debe utilizarse localmente.)
	Directory Server	4-5	Obligatoria: almacena y permite la búsqueda de datos del usuario.	
Proxy Rewriter	Portal Server	5	Obligatoria: admite la función de proxy Rewriter.	
Proxy Netlet	Portal Server	5	Obligatoria: admite la función de proxy Netlet.	
Service RegistryImplementación de Service Registry	Application Server	5	Obligatoria: proporciona servicios de tiempo de ejecución de contenedores.	Sólo local
	Java DB	5	Obligatoria: proporciona una base de datos predeterminada para almacenar servicios y metadatos relacionados.	Sólo local
	Cliente de Service Registry	5	Obligatoria: proporciona las bibliotecas de cliente necesarias.	Sólo local
Cliente de	Ninguna			

Tabla 1-8 Dependencias entre los componentes de productos de Java ES (*continúa*)

Componente de producto de la Versión 5	Dependencia ¹	Versión de Java ES	Naturaleza de la dependencia	Características
Sun Cluster	Ninguna			
Sun Cluster Agents	Sun Cluster	4-5	Obligatoria: proporciona acceso a los servicios de Sun Cluster.	Sólo local
Sun Cluster Geographic Edition	Sun Cluster	4-5	Obligatoria: admite la funcionalidad de Sun Cluster Geographic Edition.	Sólo local
Web Proxy Server	Directory Server	2-5	Opcional: proporciona autenticación basada en LDAP.	
	Web Server	2-5	Codependencia: da como resultado mejoras en la seguridad y en el rendimiento para las solicitudes HTTP. Proporciona datos a Web Proxy Server.	También se admiten: - Weblogic ² - WebSphere ³
Web Server	Directory Server	1-5	Opcional: proporciona autenticación basada en LDAP.	
	Web Proxy Server	1-5	Codependencia: da como resultado mejoras en la seguridad y en el rendimiento para las solicitudes HTTP. Distribuye la carga y los datos de la caché de Web Server.	

1. Las dependencias se muestran en el orden en el que se actualizarían normalmente para cada componente de producto.

2. BEA Weblogic Server

3. IBM WebSphere Application Server

Directrices generales de secuenciación

La elección entre una actualización selectiva o una actualización completa, las relaciones de dependencia de actualización fuertes y otros factores descritos en las secciones anteriores pueden afectar a los componentes de Java ES que desee actualizar, así como al orden de actualización de dichos componentes. No obstante, pueden utilizarse algunas directrices generales de secuenciación, aunque no en todos los casos.

La siguiente lista indica el orden en que pueden actualizarse con éxito los componentes de Java ES en un mismo equipo o en un sistema implementado. Al planificar la actualización, puede omitir aquellos componentes que no formen parte de su arquitectura de implementación o, si realiza una actualización selectiva, puede omitir los componentes que presenten relaciones de dependencia de actualización leves.

Los capítulos de esta *Guía de actualización* están organizados de acuerdo con el orden en el que aparecen los componentes en la siguiente lista.

NOTAL Antes de actualizar los componentes de Java ES, asegúrese de aplicar las actualizaciones necesarias del sistema operativo (consulte [“Revisiones del sistema operativo necesarias” en la página 46](#)).

Consulte también [“Casos especiales” en la página 61](#) para comprobar si alguno de los casos descritos se aplica a su escenario de actualización.

1. Componentes compartidos (consulte el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#))

Los componentes compartidos deben actualizarse antes que los componentes que dependen de ellos. En la mayoría de los casos, el programa de instalación de Java ES administra los componentes compartidos; sin embargo, en el caso de Web Proxy Server y Portal Server, debe actualizar de forma explícita los componentes compartidos.

2. Software de Sun Cluster (consulte el [Capítulo 3, “Software de Sun Cluster” en la página 81](#))

Si un componente se ejecuta en un entorno de Sun Cluster y es necesario actualizar el software de Sun Cluster, éste debe actualizarse antes que los componentes que utilicen los servicios de Sun Cluster. Sun Cluster Agents, en caso de actualizarse, debe incluirse como parte de la actualización de Sun Cluster.

3. Software de Sun Cluster Geographic Edition (consulte el [Capítulo 4, “Sun Cluster Geographic Edition” en la página 95](#))

Sun Cluster Geographic Edition debe actualizarse después que el software de Sun Cluster del que depende. Debería actualizarse antes que cualquiera de los componentes que utilicen los servicios de Sun Cluster.

4. Directory Server (consulte el [Capítulo 5, “Directory Server” en la página 107](#))

Muchos componentes almacenan datos del usuario o de configuración en Directory Server, por lo que la actualización de Directory Server debe realizarse, por lo general, antes que la actualización de los componentes que presentan relaciones de dependencia de configuración o tiempo de ejecución con Directory Server.

5. Directory Proxy Server (consulte el [Capítulo 6, “Directory Proxy Server” en la página 125](#))

Directory Proxy Server presenta una relación de dependencia de actualización leve con Directory Server y puede actualizarse en cualquier momento. Es posible que algunos componentes accedan a Directory Server mediante Directory Proxy Server; sin embargo, si se actualiza Directory Proxy Server, esta actualización debe realizarse justo después que la de Directory Server.

6. Web Server (consulte el [Capítulo 7, “Web Server” en la página 141](#))

Una serie de componentes de Java ES requieren compatibilidad con un contenedor web. Por lo tanto, el contenedor debe actualizarse antes que los componentes que necesitan servicios de contenedor web. Normalmente, estos servicios los proporciona Web Server o Application Server, pero si en la arquitectura se incluyen ambos, actualice primero Web Server antes que Application Server.

7. Java DB (consulte el [Capítulo 8, “Java DB” en la página 171](#))

Java DB debe actualizarse antes que Application Server, ya que esta aplicación necesita Java DB como base de datos predeterminada. No obstante, el programa de instalación de Java ES actualiza automáticamente Java DB al actualizar Application Server.

8. Almacén de sesión de alta disponibilidad (consulte el [Capítulo 9, “Almacén de sesión de alta disponibilidad” en la página 179](#))

El Almacén de sesión de alta disponibilidad (HADB) debe actualizarse antes que Application Server, ya que éste necesita este almacén para obtener alta disponibilidad. No obstante, el programa de instalación de Java ES actualiza automáticamente HADB al actualizar Application Server.

9. Message Queue (consulte el [Capítulo 10, “Message Queue” en la página 193](#))

Message Queue debe actualizarse antes que Application Server, ya que éste necesita que Message Queue sea compatible con Java Enterprise Edition (Java EE). No obstante, el programa de instalación de Java ES actualiza automáticamente Message Queue al actualizar Application Server.

10. Application Server (consulte el [Capítulo 11, “Application Server” en la página 219](#))

Application Server depende de Message Queue y el Almacén de sesión de alta disponibilidad y, si se actualiza, debe hacerlo después de actualizar estos componentes. Application Server puede depender también de Web Server para el complemento de equilibrado de carga, por lo que si utiliza esta función, Application Server debe actualizarse después de actualizar Web Server.

11. Service Registry (consulte el [Capítulo 12, “Service Registry” en la página 249](#))

Service Registry puede actualizarse en cualquier momento después de actualizar Application Server, ya que Service Registry depende de Application Server para los servicios de tiempo de ejecución de contenedores.

12. Web Proxy Server (consulte el [Capítulo 13, “Web Proxy Server” en la página 263](#))

Web Proxy Server puede actualizarse en cualquier momento, aunque normalmente se debería actualizar después del componente Web Server o Application Server, ya que proporciona un servicio de proxy. Web Proxy Server es un nuevo componente de Java ES Versión 5 que puede actualizarse desde la versión anterior, no asociada a Java ES.

13. Access Manager (consulte el [Capítulo 14, “Access Manager” en la página 281](#))

Access Manager desempeña un papel central en la autenticación y autorización, incluido el inicio de sesión único, y debe actualizarse antes que los componentes que dependen de él para poder utilizar estos servicios.

14. Portal Server (consulte el [Capítulo 15, “Portal Server” en la página 337](#))

Portal Server depende de muchos de los componentes anteriores (Directory Server, un contenedor web y Access Manager) y, si se actualiza, debería hacerlo después de actualizar estos componentes.

15. Portal Server Secure Remote Access (consulte el [Capítulo 16, “Portal Server Secure Remote Access” en la página 411](#))

Portal Server Secure Remote Access debe actualizarse al actualizar Portal Server.

Casos especiales

A continuación se describen unos pocos casos especiales que debe tener en cuenta al planificar la actualización de los componentes de Java ES a la Versión 5.

Actualización selectiva: no se actualiza Application Server

Si realiza una actualización selectiva de cualquier componente de Java ES a Java ES 5 en un equipo en el que se estén ejecutando la Versión 3 o la Versión 4 de Application Server (8.1) y no actualiza Application Server a la Versión 5, se producirán situaciones que deberán solucionarse para que Application Server siga funcionando correctamente:

- **Errores de compilación de JSP.** Antes de realizar la actualización selectiva, debería aplicar primero la revisión de Application Server que se muestra en la siguiente tabla.

Tabla 1-9 Revisiones ¹ necesarias cuando no se actualiza Application Server a la Versión 5

Descripción	Id. de revisión: Solaris 9 y 10	Id. de revisión: Linux
Solución para la Versión 3 y la Versión 4 de Application Server	119166-17 (SPARC) 119166-17 (x86)	119168-17

1. Los números de revisiones suponen la revisión mínima necesaria. Si aparecen revisiones más recientes, utilice las nuevas en lugar de las que aparecen en la tabla.

Si falla la aplicación de la revisión, Application Server experimentará errores de compilación de JSP. (Las revisiones que aparecen en la [Tabla 1-9](#) pueden aplicarse también de forma retroactiva para solucionar el problema.)

- **Reubicación de los archivos binarios del componente compartido ANT en Linux.** La Versión 5 de ANT se ubica en una ruta diferente en relación con las versiones anteriores. La variable de entorno de Application Server, especificada en el archivo *AppServer8-base/config/asenv.conf*, que señala a ANT debe cambiarse de:

```
AS_ANT_LIB="/opt/sun/lib"
```

por:

AS_ANT_LIB="/opt/sun/share/lib"

y debe reiniciarse a continuación Application Server.

Actualización de Portal Server de la Versión intermedia (IFR) 7.0 a Java ES 5

Si actualiza Portal Server en un entorno de Web Server de la Versión intermedia (IFR) 7.0 2005Q4 a la Versión 5, consulte [“Actualización de Portal Server desde la Versión intermedia 7.0” en la página 391](#) para conocer las excepciones a las directrices que aparecen en [“Directrices generales de secuenciación” en la página 57](#).

Actualización a Java ES 5 y zonas de Solaris 10

En esta sección, se describen los problemas relacionados con la actualización del software de Java ES en las zonas de Solaris 10 y se proporciona recomendaciones para dicho entorno. Esta sección sirve como complemento a la información sobre Java ES 5 y las zonas de Solaris 10 incluida en *Guía de planificación de la instalación de Java Enterprise System 5*, <http://docs.sun.com/doc/819-5079>.

Incluye los siguientes temas:

- [Compatibilidad con las zonas en el programa de instalación de Java ES](#)
- [Procedimientos de actualización recomendados](#)
- [Casos especiales o excepciones](#)

Compatibilidad con las zonas en el programa de instalación de Java ES

El programa de instalación de Java ES 5 proporciona compatibilidad completa con las zonas para la actualización (así como la instalación) de los componentes de productos de Java ES y para la sincronización de los componentes compartidos. Se han implementado las directivas en el programa de instalación para evitar escenarios de actualización problemáticos.

Actualización de los componentes de productos

Como se describe en [“Uso de la función de actualización del programa de instalación de Java ES” en la página 34](#), el programa de instalación de Java ES puede utilizarse para actualizar un número limitado de componentes de productos y sus correspondientes componentes compartidos. La función de actualización se aplica tanto a las zonas globales como a todas las zonas no globales.

Sin embargo, existen excepciones a este comportamiento relacionadas con las zonas:

- En las zonas raíz dispersas, no se pueden instalar ni actualizar algunos componentes compartidos debido a que residen en directorios de sólo lectura. En esos casos, la actualización de los componentes de productos se detiene hasta que se instalen o actualicen esos componentes compartidos en la zona global. El programa de instalación proporciona el siguiente mensaje: “Los siguientes componentes compartidos necesarios para los componentes que ha seleccionado no se pueden instalar ni actualizar en una zona raíz dispersa. Instale o actualice estos componentes compartidos en la zona global para poder continuar. Use la opción Todos los componentes compartidos.”
- Tanto Application Server como Message Queue se incluyen en el sistema operativo Solaris. Ninguna de estas versiones se puede actualizar directamente en una zona raíz dispersa. Para obtener información sobre estos dos componentes integrados, consulte [“Casos especiales de los componentes de productos” en la página 66](#).
- En una zona global, si no hay zonas no globales presentes, en lugar de actualizar todos los componentes compartidos instalados actualmente e instalar aquéllos que faltan, necesarios para el componente seleccionado, el programa de instalación sincroniza *todos* los componentes compartidos de Java ES a la Versión 5, independientemente de si son necesarios para un componente de producto específico. Este procedimiento permite que se propaguen todos los componentes compartidos de la Versión 5 a las zonas no globales, garantizando así que no habrá una combinación de diferentes versiones de los componentes compartidos en las zonas no globales.

NOTA Hay una serie de casos especiales o excepciones que puede interferir en la instalación o actualización de los componentes de productos en las zonas no globales. Estos casos se describen en [“Casos especiales o excepciones” en la página 66](#).

Sincronice todos los componentes compartidos

La opción de sincronización de todos los componentes compartidos se proporciona en la Versión 5 para abordar las situaciones en las que deban sincronizarse todos estos componentes a la Versión 5. Si se selecciona la opción Todos los componentes compartidos, el programa de instalación actualizará todos los componentes compartidos instalados actualmente e instalará los que falten, independientemente de si son necesarios para un componente de producto específico. Esta opción se aplica tanto a las zonas globales como a las zonas raíz completas (pero no a las zonas raíz dispersas).

La opción Todos los componentes compartidos, descrita más detalladamente en “[Sincronización de todos los componentes compartidos](#)” en la [página 72](#), es necesaria en los dos siguientes escenarios de actualización basada en zonas:

- **Actualización manual de los componentes de productos.** La opción Todos los componentes compartidos es necesaria para realizar la instalación y actualización de los componentes compartidos necesarios al actualizar los componentes de productos que *no se pueden* actualizar mediante el programa de instalación de Java ES.
- **Actualización en una zona raíz dispersa.** Algunos componentes compartidos no se pueden instalar ni actualizar en las zonas raíz dispersas predeterminadas. Por lo tanto, al utilizar el programa de instalación de Java ES para actualizar los componentes de productos en las zonas raíz dispersas, es posible que sea necesario sincronizar los componentes compartidos en la zona global en función de los componentes compartidos relacionados con este proceso. Puede utilizar la opción Todos los componentes compartidos en la zona global para realizar la instalación y la actualización de los componentes compartidos necesarios en este caso.

Para obtener un resumen del comportamiento de las zonas del programa de instalación de Java ES en relación con los componentes compartidos, consulte la información sobre Java ES 5 y las zonas de Solaris 10 en *Guía de planificación de la instalación de Java Enterprise System 5*, <http://docs.sun.com/doc/819-5079>.

Procedimientos de actualización recomendados

Al elaborar un plan de actualización, debería comprobar si existen implementaciones multizona del software de Java ES, teniendo en cuenta las estrategias de administración e instalación de zonas descritas en la *Guía de planificación de la instalación de Java Enterprise System 5*, <http://docs.sun.com/doc/819-5079>. En algunos casos, es posible que sea necesario desinstalar componentes en una o varias zonas y reinstalarlos en otras zonas para implementar los siguientes procedimientos recomendados:

- Evite combinar diferentes estrategias. En concreto:
 - Simplifique al máximo su estrategia de administración e implementación de las zonas de Java ES. No mezcle implementaciones de los componentes de Java ES en zonas raíz dispersas y completas en un mismo equipo. (Los procedimientos y las tareas necesarias para poder utilizar las implementaciones en zonas raíz dispersas pueden interferir en las implementaciones en zonas raíz completas.)
 - No instale el mismo componentes de Java ES tanto en la zona global como en las zonas no globales, aunque sean de versiones diferentes. (Los procedimientos necesarios para actualizar una instalación en la zona global pueden interrumpir las instalaciones en las zonas no globales.)
 - Cuando los componentes de la Versión 4 (o anterior) de Java ES se hayan instalado en una zona raíz completa, no actualice los componentes de Java ES a la Versión 5 en la zona global. La actualización en la zona global podría dar como resultado una combinación de archivos de la Versión 4 y la Versión 5 en la zona raíz completa.
- Procedimientos de actualización:
 - Si desea actualizar todos los componentes de productos instalados de la Versión 4 a la Versión 5, sincronice todos los componentes compartidos de Java ES en la zona global y, a continuación, realice la actualización de los componentes de productos que desee en las zonas en las que se hayan instalado. (Los componentes compartidos de la Versión 5 son compatibles con las versiones anteriores.)
 - Si tiene componentes de productos de la Versión 4 o la Versión 5 instalados en un entorno sin zonas, desea agregar zonas no globales al entorno e instalar los componentes de productos en las nuevas zonas no globales, es posible que deba desinstalar los componentes de la zona global y reinstalarlos en las zonas no globales.

Casos especiales o excepciones

Existen varios casos especiales, algunos de los cuales surgen del hecho de que algunos componentes compartidos de Java ES y algunos componentes de productos de Java ES se incluyen en Solaris 10. Debido a esta integración, estos componentes de Java ES residen automáticamente en la zona global y, por lo tanto, en cualquier zona no global que se haya creado desde la zona global.

Casos especiales de los componentes de productos

- **Message Queue.** Message Queue se incluye en Solaris 10 y, por lo tanto, se propaga automáticamente al crear las zonas no globales (a menos que se haya eliminado primero Message Queue de la zona global). Message Queue no puede instalarse ni actualizarse en una zona raíz dispersa. Cuando el programa de instalación de Java ES realiza la instalación o la actualización en una zona global, Message Queue, a diferencia de los demás componentes de productos, se propaga de forma predeterminada a las zonas no globales.
- **Application Server.** Application Server se incluye en Solaris 10 y, por lo tanto, se propaga automáticamente al crear las zonas no globales (a menos que se haya eliminado primero Application Server de la zona global). Cuando se propaga de esta forma, la instancia integrada de Application Server, que se ha instalado en /usr, no se puede actualizar mediante el programa de instalación de Java ES en una zona raíz dispersa (/usr es de forma predeterminada un directorio de sólo lectura). Para solucionar este problema, los paquetes de Application Server integrados deben eliminarse manualmente de la zona global antes de instalar la Versión 5 de Application Server en una zona raíz dispersa. Consulte el [“Sólo para Solaris: Elimine manualmente los paquetes de Application Server integrados con el sistema operativo” en la página 237](#).
- **Sun Cluster.** El software de Sun Cluster no se admite en las zonas no globales.

Casos especiales de los componentes compartidos

- **Sun Java Web Console (SJWC).** El programa de instalación de Java ES no puede eliminar los paquetes de SJWC incluidos en Solaris 10 (Update 1 y Update 2). En estos paquetes antiguos de SJWC, el atributo SUNW_PKG_ALLZONES se establece en True (verdadero), lo que implica que el paquete debe ser idéntico en todas las zonas y sólo lo puede administrar el administrador global. Por lo tanto, deben eliminarse manualmente estos paquetes en la zona global y sustituirse por los paquetes correctos.

Si el programa de instalación de Java ES intenta instalar un componente de producto seleccionado en una zona no global y detecta que SJWC debe actualizarse, el programa de instalación se bloqueará. Esta situación se producirá al realizar la instalación en Solaris 10, Update 1 y 2.

Para solucionar este problema, se ha desarrollado una secuencia de comandos que eliminará los paquetes antiguos de SJWC de la zona global y los sustituirá por la Versión 5, que presenta el valor correcto del atributo de propagación de zonas. Consulte *Guía de instalación de Java Enterprise System 5 para UNIX* para obtener más información.

- **Contenedor de agentes común (CAC).** La versión 1.1 sólo se instala al instalar Sun Cluster, Sun Cluster Geographic Edition o Sun Cluster Agents. Sin embargo, no se instala si se ha seleccionado la opción Todos los componentes compartidos. En ese caso, sólo se instala la versión 2.0.
- **Sun Explorer Data Collector.** Este componente compartido sólo se instala al instalar Sun Cluster, Sun Cluster Geographic Edition o Sun Cluster Agents. Sin embargo, no se instala si se ha seleccionado la opción Todos los componentes compartidos.

Actualización de los componentes compartidos de Java ES

En este capítulo se proporciona información sobre la actualización de los componentes compartidos de Java ES a Java ES 5 (Versión 5).

Cada componente de producto de Java ES depende de una o varias bibliotecas compartidas localmente, conocidas como componentes *compartidos* de Java ES. El programa de instalación de Java ES instala automáticamente estos componentes compartidos durante la instalación de los componentes de productos, en función de los componentes que se vayan a instalar. Éstos no se seleccionan, instalan ni configuran de forma explícita durante la implementación de los componentes de productos de Java ES.

Del mismo modo, los componentes compartidos de aquellos componentes de productos que pueden actualizarse automáticamente mediante el programa de instalación de Java ES también se actualizan automáticamente.

Sin embargo, en los casos en los que los componentes de productos tengan que actualizarse manualmente, como ya se ha descrito en varios capítulos de esta *Guía de actualización*, la actualización de los componentes compartidos debe realizarse de forma explícita utilizando los procedimientos descritos en este capítulo.

Este capítulo incluye los siguientes apartados:

- “Visión general de la actualización de componentes compartidos” en la página 70
- “Procedimiento de actualización de componentes compartidos” en la página 75
- “Procedimientos especiales de actualización” en la página 75

Visión general de la actualización de componentes compartidos

La actualización de los componentes compartidos a Java ES 5 (Versión 5) debe realizarse como parte del plan de actualización, como se describe en el [Capítulo 1, “Planificación de las actualizaciones”](#).. Para garantizar una actualización satisfactoria, lea detenidamente el capítulo 1 y prepare un plan de actualización que responda a sus necesidades.

En este apartado se describen los temas siguientes:

- [Consideraciones generales](#)
- [Sincronización de los componentes compartidos](#)
- [Sincronización de todos los componentes compartidos](#)
- [Consideraciones de la zona Solaris 10](#)

Consideraciones generales

Cuando actualice los componentes compartidos, tenga en cuenta los aspectos que se describen a continuación:

- **Problemas del sistema operativo** Realice las actualizaciones necesarias del sistema operativo, tal y como se describe en [“Consideraciones sobre el sistema operativo” en la página 46](#). En todas las plataformas, excepto en Solaris 10, actualice el sistema operativo antes de actualizar los componentes compartidos.
- **Directrices de secuenciación.** Revise las directrices de secuencias que se describen en [“Directrices generales de secuenciación” en la página 57](#). Normalmente, los componentes compartidos se actualizan en primer lugar. Sin embargo, debe conocer toda la secuencia de actualización a Java ES Versión 5 antes de comenzar el proceso de actualización.

Sincronización de los componentes compartidos

La dificultad que supone el comprobar y compatibilizar el gran número (cerca de 30) y la complejidad de las interacciones entre los componentes compartidos de Java ES y los componentes de los productos de Java ES requiere que todos los componentes compartidos de una única instancia de sistema operativo se

sincronicen en la misma versión de Java ES. Una instancia de sistema operativo significa que el sistema operativo Solaris 9 o Linux se ejecuta en un único equipo o, en el caso del sistema operativo Solaris 10, significa que cualquiera de los entornos (zonas) de un sistema operativo se ejecuta en un solo equipo.

En otras palabras, todos los componentes compartidos de Java ES instalados en una instancia de sistema operativo deben ser de la misma versión. Este requisito de sincronización supone ciertas restricciones en relación a cómo se pueden instalar y actualizar los componentes compartidos de Java ES:

- Diferentes versiones de los componentes compartidos de Java ES sólo pueden residir en instancias de sistemas operativos diferentes. Por ejemplo, puede instalar los componentes compartidos de Java ES Versión 4 en una instancia de sistema operativo y los componentes compartidos de Java ES Versión 5 en otra diferente, pero no puede combinarlos en la misma instancia.
- Si se actualiza cualquier componente compartido de una instancia de sistema operativo o se introduce un componente compartido nuevo de una versión superior, todos los componentes compartidos de esa instancia de sistema operativo deberán actualizarse al mismo tiempo. (Es necesaria la compatibilidad de los componentes compartidos con versiones anteriores, por lo que no hay ningún problema si componentes de productos de la Versión 4 trabajan con componentes compartidos de la Versión 5).

Por ejemplo, supongamos que se instala un componente de producto de la Versión 5 en una instancia de sistema operativo en la que residen uno o más componentes de productos de la Versión 4. Ya que el componente de producto de la Versión 5 requiere una serie de componentes compartidos de la Versión 5, el requisito de sincronización implica que todos los componentes compartidos de la Versión 4 que residan en esa instancia de sistema operativo deben actualizarse a la Versión 5 al mismo tiempo que se instala el componente de producto de la Versión 5. (Esto será así incluso si el componente de producto de la Versión 5 instalado requiere unos componentes compartidos diferentes de los que ya están instalados).

Del mismo modo, si se actualiza un componente de producto de la Versión 4 a la Versión 5 y esta actualización requiere que se actualicen varios componentes compartidos de los que depende, deberán actualizarse a la Versión 5 todos los componentes compartidos instalados en la instancia de ese sistema operativo, independientemente de que ese componente de producto concreto de la Versión 4 actualizado tenga relaciones de dependencia con todos ellos o no.

Sincronización de todos los componentes compartidos

El programa de instalación de Java ES incluye una función para sincronizar todos los componentes compartidos en aquellas situaciones en las que tengan que sincronizarse todos los componentes compartidos en la Versión 5.

Cuando se selecciona Todos los componentes compartidos en la página de selección de componentes del programa de instalación de Java ES, éste actualizará cualquier componente compartido existente e instalará todos los que falten, independientemente de si es necesario o no para cualquier componente de producto específico.

La función de sincronización de todos los componentes compartidos es compatible con los componentes de productos *no* actualizados explícitamente por el programa de instalación de Java ES (es decir, con todos los componentes de productos de Java ES excepto Application Server, Message Queue, HADB y Java DB). Por ejemplo, la función de sincronización de todos los componentes compartidos se utiliza para actualizar Web Proxy Server y Portal Server a la Versión 5.

Los motivos para la sincronización de *todos* los componentes compartidos en este caso son que el programa de instalación actual no sabe qué componentes compartidos tienen que sincronizarse en un equipo. Por lo tanto, esta función instala o actualiza *todos* los componentes compartidos de Java ES a la Versión 5.

La función de sincronización de todos los componentes compartidos también admite un número de escenarios de zona como se describe a continuación en [“Consideraciones de la zona Solaris 10,”](#).

Consideraciones de la zona Solaris 10

Algunas de las limitaciones de la implementación de Java ES en un entorno de zona múltiple Solaris 10 derivan de consideraciones vinculadas con los componentes compartidos.

Lo más importante de estas consideraciones es que un gran número de componentes compartidos no pueden instalarse en zonas root dispersas debido a la presencia de sistemas de archivos de sólo lectura en estas zonas. Esta limitación se aplica a aquellos componentes compartidos cuyo directorio de base es /usr (un directorio compartido de manera predeterminada por la zona global).

La incapacidad para instalar varios componentes compartidos de Java ES en zonas root dispersas significa que para instalar o actualizar satisfactoriamente componentes de productos que presenten relaciones de dependencia con dichos componentes compartidos en zonas root dispersas, los componentes compartidos deben instalarse o actualizarse primero en la zona global, desde donde se propagan a las zonas no globales.

Debido a los requisitos de sincronización relacionados con los componentes compartidos (consulte [“Sincronización de los componentes compartidos” en la página 70](#)) y a que la instalación o actualización de componentes compartidos en la zona global debe adaptarse a cualquier componente de producto que se esté instalando o actualizando en la zona root dispersa, es necesario que se sincronicen todos los componentes compartidos en las versiones de la Versión 5 en la zona global. Esto significa que hay que actualizar cualquier componente compartido existente e instalar todos los que falten, independientemente de si son necesarios para cualquier componente de producto específico en la zona root dispersa.

Esta sincronización de los componentes compartidos en la zona global puede llevarse a cabo seleccionando Todos los componentes compartidos en la página de selección de componentes del programa de instalación de Java ES.

Cuando se instalan y propagan los componentes compartidos desde la zona global (por ejemplo, instalando un componente de producto de Java ES en la zona global), es necesario prestar especial atención para que se mantenga la sincronización de los componentes compartidos en *todas* las zonas. En caso contrario, existe la posibilidad de que se mezclen los componentes compartidos de una versión anterior en una zona no global con los componentes compartidos de la Versión 5 que se han propagado desde la zona global.

Enfoques para la actualización de componentes compartidos

Existen dos enfoques para actualizar los componentes compartidos necesarios para actualizar un componente de producto particular de Java ES. El primero consiste en determinar todos los componentes compartidos necesarios e instalarlos o actualizarlos manualmente a las versiones de la Versión 5. El segundo consiste en utilizar la función del programa de instalación de Java ES para sincronizar Todos los componentes compartidos.

Sin embargo, debido al requisito de sincronización relacionado con los componentes compartidos (consulte [“Sincronización de los componentes compartidos” en la página 70](#)), el único enfoque práctico consiste en utilizar la función de sincronización de Todos los componentes compartidos del programa de instalación de Java ES.

Esto ocurre porque, en la mayoría de los casos, es muy difícil determinar qué componentes compartidos necesitan instalarse o actualizarse en un caso concreto; incluso si se hiciera satisfactoriamente, la actualización manual de los componentes compartidos necesarios no es trivial. Algunos componentes compartidos pueden modificarse en la Versión 5, pero algunos requieren que se sustituyan los paquetes existentes por los nuevos paquetes de la Versión 5. Dependiendo de la ruta de actualización, algunos paquetes existentes deberán ser eliminados manualmente.

En el pasado, la dificultad que suponía la actualización manual de los componentes compartidos era una barrera significativa para la actualización de los componentes de productos. La función de sincronización de Todos los componentes compartidos, a pesar del inconveniente que supone el hecho de tener que instalar los componentes compartidos que no son necesarios, representa una mejora importante en relación con la actualización manual de componentes compartidos requerida en la Versión 3 y la Versión 4 de Java ES.

Procedimiento de actualización de componentes compartidos

El procedimiento para instalar componentes compartidos es utilizar la función de sincronización de Todos los componentes compartidos del programa de instalación de Java ES.

1. Inicie sesión como root o conviértase en superusuario.

```
su -
```

2. Cierre todos los servicios o procesos como se indica en [“Procedimientos especiales de actualización” en la página 75](#).

3. Inicie el programa de instalación de Java ES.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

4. Seleccione Todos los componentes compartidos en la página de selección de componentes.
5. Confirme su elección.

Todos los componentes compartidos se sincronizarán en la Versión 5.

6. Salga del programa de instalación de Java ES.

Consulte [“Procedimientos especiales de actualización” en la página 75](#) para cualquier procedimiento de seguimiento.

Procedimientos especiales de actualización

Esta sección ofrece procedimientos especiales que son necesarios para la actualización de los siguientes componentes compartidos:

- [“Procedimientos de actualización de JAVA SE” en la página 76](#)

- “Procedimientos de actualización del contenedor de agentes común” en la [página 78](#)

Procedimientos de actualización de JAVA SE

Java ES Versión 5 está certificado para Java Platform, Standard Edition (JAVA SE) Versión 5.0 Update 9, denominado aquí como JAVA SE 5.0 Update 9. (JAVA SE 5.0 recibe a veces la designación de versión del programador 1.5.0).

Si actualiza Java SE a la Versión 5.0 Update 9 con el programa de instalación de Java ES, la actualización transcurre como se describe a continuación:

- La actualización *no elimina* ninguna versión superior anteriormente instalada de Java SE (por ejemplo, Java SE Versión 1.4.2 o Java SE Versión 1.6.x), dado que es posible que otras aplicaciones dependan de esta versión. Sin embargo, durante la actualización se establece un enlace simbólico que hace referencia a la versión de la Versión 5 y que se muestra en la tabla que aparece a continuación.

Tabla 2-1 Enlace simbólico a JAVE SE según la plataforma

Plataforma	Enlaces simbólicos	Ubicación
SO Solaris	/usr/jdk/entsys-j2se	/usr/jdk/instances/jdk1.5.0
Linux	/usr/jdk/entsys-j2se	/usr/java/jdk1.5.0_09

- Cuando se actualiza, *se elimina* una versión inferior anteriormente instalada de Java SE (por ejemplo, Java SE Versión 5.0 Update 5) y se sustituye por Java SE 5.0 Update 9.

Debe mantener cualquier puntero a versiones superiores de JAVA SE (por ejemplo, JAVA SE 1.4.2) para aquellos servicios que requieran versiones anteriores. Consulte la documentación adecuada del componente de producto para obtener información sobre cómo mantener los enlaces simbólicos a las versiones anteriores de Java SE.

Al actualizar Java SE, es recomendable cerrar primero todos los servicios que dependan de la instalación actual de Java SE. De esta manera se evitará cualquier problema que pueda surgir de estos servicios. Si no cierra los servicios que dependan de Java SE, tendrá que reiniciar el sistema después de actualizar Java SE a la Versión 5.

NOTA El programa de instalación de Java ES instala Java SE 5.0 Update 9 o actualiza Java SE independientemente de que se instalen o actualicen otros componentes compartidos. No es preciso seleccionar explícitamente Todos los componentes compartidos para instalar Java SE 5.0 Update 9.

Comprobación del enlace simbólico de Java SE

Java Enterprise System mantiene un enlace simbólico a la versión admitida de la plataforma Java SE para asegurar que los servicios de Java ES pueden encontrar el tiempo de ejecución adecuado de Java SE.

Compruebe el enlace simbólico (por ejemplo, en el sistema operativo Solaris) como se indica a continuación:

```
ls -l /usr/jdk/entsys-j2se
lrwxrwxrwx 1 root  other  7 Jul 7 23:18 /usr/jdk/entsys-j2se ->
    /usr/jdk/instances/jdk1.5.0
```

donde /usr/jdk/instances/jdk1.5.0 es la ubicación predeterminada.

Verificación de la versión actual de Java SE

Para determinar qué versión de Java SE está utilizando el programa de instalación de Java ES, ejecute el siguiente comando, que verifica la versión de Java SE a la que hace referencia el enlace simbólico de Java SE:

```
/usr/jdk/entsys-j2se/bin/java -version
```

Los resultados se muestran en la siguiente tabla:

Tabla 2-2 Resultados de la verificación de la versión de Java SE

Versión de Java ES	Número de versión de Java SE	Cadena de la versión de Java SE
Versión 2	1.4.2 Update 5	1.4.2_05
Versión 3	5.0 Update 1	1.5.0_01
Versión 4	5.0 Update 4	1.5.0_04
Componente de producto de la	5.0 Update 9	1.5.0_09

Procedimientos de actualización del contenedor de agentes común

Si va a actualizar los componentes compartidos del contenedor de agentes común como preparación para la actualización del software de Sun Cluster, (es decir, aplicación de revisiones en la versión 1.1), siga los procedimientos de actualización del software de dependencia de la sección “Actualización del software de Sun Cluster” de la *Sun Cluster Guía de instalación para el sistema operativo Solaris*, <http://docs.sun.com/doc/819-0420/6n2rlnnrc?a=view>.

Para más información sobre actualizaciones de la guía anterior, consulte “Upgrading to Sun Cluster 3.1 8/05 Software” de *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>.

Si va a actualizar los componentes compartidos del contenedor de agentes común como preparación para la actualización de otros componentes de Java ES (es decir, actualización a la versión 2.0), siga los procedimientos de actualización descritos a continuación, prestando atención a las siguientes variables del nombre de ruta:

Tabla 2-3 Rutas de directorio del contenedor de agentes común

Variable de nombre de ruta	SO Solaris	SO Linux
<i>rel4CACbase-dir</i>	/opt/SUNWcacao	/opt/sun/cacao
<i>rel5CAC-admin-dir</i>	/usr/lib/cacao	/opt/sun/cacao

1. Si la instalación actual utiliza valores de configuración personalizados, capture los valores de configuración mediante los siguientes comandos:

```
rel4CAC-base-dir/bin/cacaoadm list-params
```

El resultado debería ser similar al siguiente:

```
java-flags=-Xms4M -Xmx64M
jmxmp-connector-port=10162
snmp-adaptor-port=10161
snmp-adaptor-trap-port=10162
commandstream-adaptor-port=10163
retries=4
```

El ejemplo anterior muestra los valores predeterminados. Anote todos los valores de configuración no predeterminados para utilizarlos en el [Paso 4 en la página 79](#).

2. Detenga los procesos del contenedor de agentes común mediante los siguientes comandos:

```
rel4CAC-base-dir/bin/cacaoadm stop
echo $?
```

Si el código de salida no es 0, deberá detenerse forzosamente:

```
rel4CAC-base-dir/bin/cacaoadm stop -f
```

3. Actualice el contenedor de agentes común mediante la función de sincronización de Todos los componentes compartidos del programa de instalación de Java ES.

Consulte el [“Procedimiento de actualización de componentes compartidos” en la página 75](#).

4. Aplique los parámetros de configuración personalizados capturados anteriormente en el [Paso 1 en la página 78](#).

```
rel5CAC-admin-dir/bin/cacaoadm set-param java-flags=Value
rel5CAC-admin-dir/bin/cacaoadm set-param jmxmp-connector-port=Value
rel5CAC-admin-dir/bin/cacaoadm set-param snmp-adaptor-port=Value
rel5CAC-admin-dir/bin/cacaoadm set-param
snmp-adaptor-trap-port=Value
rel5CAC-admin-dir/bin/cacaoadm set-param
commandstream-adaptor-port=Value
rel5CAC-admin-dir/bin/cacaoadm set-param retries=Value
```

5. Si ha actualizado Java SE a Java SE Versión 5, ejecute la utilidad para reconstruir las dependencias:

```
rel5CAC-admin-dir/bin/cacaoadm rebuild-dependencies
```

El resultado de este comando será el siguiente:

```
Property updated: [java-home].
Property updated: [jdmk-home].
Property updated: [nss-lib-home].
Property updated: [nss-tools-home].
```

6. Reinicie los servicios del contenedor de agentes común:

```
rel5CAC-admin-dir/bin/cacaoadm stop
rel5CAC-admin-dir/bin/cacaoadm start
```

7. Verifique la actualización del contenedor de agentes común:

```
rel5CAC-admin-dir/bin/cacaoadm status
rel5CAC-admin-dir/bin/cacaoadm verify-configuration
```


Software de Sun Cluster

En este capítulo se describe cómo actualizar el software de Sun Cluster a Java ES 5 (Versión 5): software de Sun Cluster 3.1 8/05 .

Este capítulo proporciona una visión general de las consideraciones que es preciso tener en cuenta en la actualización del software de Sun Cluster a la Versión 5.

El software de Sun Cluster sólo se admite en las plataformas Solaris.

El proceso de actualización del software de Sun Cluster descrito en este capítulo incluye tanto el software de la estructura de Sun Cluster como el software de los servicios de datos, o agentes, de Sun Cluster.

- “Visión general de la actualización del software de Sun Cluster” en la página 82
- “Actualización del software de Sun Cluster a Java ES Versión 5” en la página 86

Visión general de la actualización del software de Sun Cluster

En esta sección se describen los siguientes aspectos generales de Sun Cluster que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca del software de Sun Cluster de la Versión 5](#)
- [Guía de actualización del software de Sun Cluster](#)
- [Datos de Sun Cluster](#)
- [Estrategia de actualización para Sun Cluster](#)

Acerca del software de Sun Cluster de la Versión 5

El software de Sun Cluster de la Versión 5 representa una actualización inferior con respecto al software de la Versión 4 de Sun Cluster (consulte las *Sun Cluster Release Notes*, <http://docs.sun.com/doc/819-1405/6n3p13hac?a=view>). La Versión 5 de Sun Cluster es prácticamente la misma que la Versión 4, salvo que la Versión 5 no admite el sistema operativo Solaris 8.

Para más información sobre cambios y adiciones en el conjunto de documentación de Sun Cluster 3.1 8/05, consulte *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>. De lo contrario, son válidos los procedimientos descritos en el conjunto de documentación de Sun Cluster 3.1 8/05 para el software de la Versión 5 de Sun Cluster.

NOTA

Si necesita Sun Cluster 3.1 8/05 en el SO Solaris 8, debe obtener el software de Sun Cluster 3.1 8/05 de la distribución de Java ES Versión 4, que se encuentra en <http://www.sun.com/software/javaenterprisesystem/previous/index.xml>.

La instalación del software de Sun Cluster 3.1 8/05 en el SO Solaris 8 ya no es admitida por el programa de instalación de Java ES 5.

Para instalar el software de Sun Cluster 3.1 8/05 en el SO Solaris 8, siga los pasos que se describen a continuación:

1. Instale el software de Sun Cluster 3.1 8/05 desde la distribución de Java ES Versión 4.
2. Instale todas las revisiones necesarias para el software de Sun Cluster 3.1 8/05.

Guía de actualización del software de Sun Cluster

La [Tabla 3-1](#) muestra las rutas de actualización compatibles con Sun Cluster para Java ES 5 (Versión 5). Esta tabla sólo se puede aplicar al sistema operativo Solaris.

Las versiones de Sun Cluster no se asignan de forma individualizada a las versiones de Java ES. En el pasado se incorporaron versiones intermedias (Interim Feature Release, IFR) del software de Sun Cluster en Java ES entre las versiones convencionales de Java ES. Por este motivo, la actualización de Java ES Versión 2, Versión 3 y Versión 4 de Sun Cluster a la Versión 5 de Sun Cluster, como se muestra en la [Tabla 3-1](#), incluye la actualización del software de Sun Cluster 3.1 4/04, Sun Cluster 3.1 9/04 y Sun Cluster 3.1 8/05 a la Versión 5.

Tabla 3-1 Rutas de actualización a Java ES 5 (Versión 5): Software de Sun Cluster 3.1 8/05

Versión de Java ES	Sun Cluster Versión del software	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Cluster 3.1 8/05 (2005Q4)	Actualización directa ¹ : Se realiza mediante la utilidad scinstall de Sun Cluster.	None (Ninguna).

Tabla 3-1 Rutas de actualización a Java ES 5 (Versión 5): Software de Sun Cluster 3.1 8/05

Versión de Java ES	Sun Cluster Versión del software	Enfoque general	Reconfiguración necesaria
Versión 3	Sun Cluster 3.1 9/04 o Sun Cluster 3.1 8/05 (IFR)	Actualización directa: Se realiza mediante la utilidad scinstall de Sun Cluster.	La configuración del clúster se migra automáticamente a la versión actualizada. No se requiere ninguna reconfiguración al actualizar IFR a la Versión 5.
Versión 2	Sun Cluster 3.1 4/04 o Sun Cluster 3.1 9/04 (IFR)	Actualización directa: Se realiza mediante la utilidad scinstall de Sun Cluster.	La configuración del clúster se migra automáticamente a la versión actualizada.
Versión 1	Sun Cluster 3.1	Actualización directa no certificada: Aunque puede realizarse mediante la utilidad scinstall.	La configuración del clúster se migra automáticamente a la versión actualizada.
Versiones anteriores de Java ES	Sun Cluster 3.0	Actualización directa no certificada: Aunque puede realizarse mediante la utilidad scinstall.	La configuración del clúster se migra automáticamente a la versión actualizada.

1. La actualización de la Versión 4 a la Versión 5 no es necesaria, a no ser que los componentes compartidos utilizados por el software de Sun Cluster hayan sido actualizados a la Versión 5.

Datos de Sun Cluster

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Sun Cluster.

Tabla 3-2 Uso de datos de Sun Cluster

Tipo de datos	Ubicación	Uso
Datos de configuración del clúster	El depósito de configuración del clúster, que se replica y sincroniza en todos los nodos del clúster. (ADVERTENCIA: no edite nunca manualmente los archivos CCR, ya que un nodo o todo el clúster podría dejar de funcionar.)	Almacena información de configuración sobre todos los aspectos relacionados con las operaciones de Sun Cluster: configuración de los nodos del clúster, mecanismos de conmutación por error, administración de recursos, etc.

Estrategia de actualización para Sun Cluster

La estrategia utilizada para la actualización de Sun Cluster depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Sun Cluster presentando una serie de problemas que pueden influir en el plan de actualización de Sun Cluster.

Problemas de compatibilidad

El software de Sun Cluster de Java ES Versión 5 incluye nuevas interfaces gráficas de administración, aunque es compatible con las versiones anteriores de los agentes de Sun Cluster.

Sun Cluster Dependencias

Las dependencias de Sun Cluster con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Sun Cluster. Por ejemplo, los cambios en las interfaces y las funciones de Sun Cluster pueden requerir las versiones actualizadas de los componentes de los que depende el software de Sun Cluster. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Sun Cluster presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** El software de Sun Cluster presenta dependencias en relación con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Servicios de datos.** El software de Sun Cluster requiere que determinados servicios de datos (o agentes) conviertan a los componentes de productos de Java ES en altamente disponibles. Para cada componente de producto que se ejecute en un entorno de Sun Cluster, debe haber un servicio de datos con el fin de administrar los recursos del clúster correspondientes. Los paquetes de agentes se actualizan normalmente como parte del proceso de actualización de Sun Cluster.

Actualización del software de Sun Cluster a Java ES Versión 5

En esta sección se incluye información sobre la actualización del software de Sun Cluster desde Java ES 2005Q4 (Versión 4), Java ES 2005Q1 (Versión 3) y Java ES 2004Q2 (Versión 2) a Java ES 5 (Versión 5). El procedimiento de actualización es el mismo para las tres versiones de Sun Cluster incluidas en estas versiones de Java ES: el software de Sun Cluster 3.1 4/04, Sun Cluster 3.1 9/04 y Sun Cluster 3.1 8/05.

Si ya tiene instalado el software de Sun Cluster 3.1 8/05 (Versión 3 o Versión 4), no es necesario que lo actualice a la Versión 5, a no ser que los componentes compartidos utilizados por el software de Sun Cluster hayan sido actualizados a la Versión 5.

En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de Sun Cluster](#)

Introducción

Al actualizar el software de Sun Cluster a Java ES Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque de actualización general.** Para realizar la actualización, se debe ejecutar la secuencia de comandos `scinstall`, que actualiza el software Sun Cluster y aplica la configuración anterior de Sun Cluster una vez completada la actualización. No obstante, deben actualizarse todos los nodos de un clúster a la misma versión. Para ello, se puede cerrar el clúster y actualizar todos los nodos, o realizar una actualización por turnos mediante la que se actualicen todos los nodos sucesivamente sin necesidad de cerrar el clúster.
- **Dependencias de actualización.** Aunque el software de Sun Cluster tiene relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)), estas relaciones de dependencia son leves: El software de Sun Cluster de Java ES Versión 5 es compatible con las versiones de los componentes de la Versión 4.

- **Compatibilidad con versiones anteriores.** La Versión 5 del software de Sun Cluster (estructura) es compatible con los agentes del clúster anteriores y el software del agente de la Versión 5 de Sun Cluster es compatible con los componentes de Java ES Versión 4. Sin embargo, todos los nodos del clúster deben ejecutar la misma versión del software del agente y la estructura.
- **Anulación de la actualización.** No se puede deshacer la actualización al software de Sun Cluster de la Versión 5 para restablecer las versiones anteriores.
- **Problemas de plataforma.** El enfoque de actualización del software de Sun Cluster es igual en todas las plataformas Solaris y arquitecturas de hardware. Sin embargo, no se admite el software de Sun Cluster en las plataformas Linux.

Actualización de Sun Cluster

En esta sección se proporciona una visión general de cómo realizar una actualización del software de Sun Cluster de Java ES Versión 4 a Java ES Versión 5:

- [Tareas previas a la actualización](#)
- [Actualización del software de Sun Cluster](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

En esta sección se describe una actualización de Sun Cluster conjunta. La actualización por turnos es ligeramente distinta, ya que no es necesario cerrar el clúster. Sin embargo, en ambos casos, se deben realizar los mismos procedimientos generales descritos a continuación para un determinado nodo del clúster. Para conocer los procedimientos específicos, consulte el capítulo sobre actualización de *Sun Cluster Installation Guide*, <http://docs.sun.com/doc/819-0420/6n2rlnnr?a=view>. Las modificaciones para la Versión 5 de Sun Cluster se describen en *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>.

Tareas previas a la actualización

Antes de actualizar el software de Sun Cluster, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)

- [Prepare el nodo del clúster para la actualización](#)
- [Actualice el sistema operativo](#)
- [Actualización de las dependencias de Sun Cluster](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual del software de Sun Cluster, introduzca el siguiente comando:

```
scinstall -pv
```

El comando devuelve la versión del software de Sun Cluster y de cada paquete de software instalado. Si este comando devuelve la versión 3.1 8/05, 3.1u4, entonces compruebe los números de revisiones para ver si tiene instalado el software de la Versión 4 o de la Versión 5, como se indica en la siguiente tabla.

Tabla 3-3 Sun Cluster Resultados de la verificación de la versión

Versión de Java ES	Número de versión de Sun Cluster	Números de revisiones
Versión 1 (Sun Cluster 3.1)	3.1	
Versión 2 (Sun Cluster 3.1 4/04)	3.1u2	
Versión 2 ó 3 (Sun Cluster 3.1 9/04)	3.1u3	
Versión 3 ó 4 (Sun Cluster 3.1 8/05)	3.1u4	Solaris 9 sparc: 117949-15 Solaris 8 sparc: 117950-15 Solaris 9 x86: 117909-15
Versión 5 (Sun Cluster 3.1 8/05)	3.1u4	Solaris 10 sparc: 120500-08 ¹ Solaris 9 sparc: 117949-23 Solaris 8 sparc: 117950-23 Solaris 10 x86: 120501-08 Solaris 9 x86: 117909-23

1. Los números de revisiones suponen la revisión mínima requerida para actualizar a Java ES Versión 5 para las diferentes plataformas. Si aparecen revisiones más recientes, utilice las nuevas en lugar de las que aparecen en la tabla.

Prepare el nodo del clúster para la actualización

El nodo del clúster debe eliminarse del entorno del clúster antes de poder actualizar el software de Sun Cluster:

- **Actualización conjunta.** Para eliminar el nodo del entorno del clúster, se debe cerrar el entorno: se debe desconectar y desactivar los grupos de recursos, cerrar las aplicaciones que se ejecuten en el entorno, realizar una copia de seguridad de los datos compartidos, cerrar el clúster, realizar una copia de seguridad del disco del sistema y reiniciar el nodo en el modo sin clúster.

- **Actualización por turnos** Para eliminar el nodo del entorno del clúster, se deben mover todos los grupos de recursos y dispositivos del nodo, realizar una copia de seguridad de los datos compartidos y el disco del sistema y reiniciar el nodo en el modo sin clúster.

Puede encontrar información sobre estas operaciones y otras que es posible que deban realizarse en situaciones específicas en el capítulo sobre la actualización de la *Sun Cluster Installation Guide*,
<http://docs.sun.com/doc/819-0420/6n2rlnnrc?a=view>.

Actualice el sistema operativo

Es recomendable aprovechar el tiempo de inactividad para actualizar el sistema operativo a la versión más actual y la versión del administrador de volúmenes que se esté utilizando.

Para obtener información detallada sobre estas operaciones, consulte el capítulo sobre actualización de la *Sun Cluster Installation Guide*,
<http://docs.sun.com/doc/819-0420/6n2rlnnrc?a=view>.

Actualización de las dependencias de Sun Cluster

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a la Versión 5. La actualización de los componentes compartidos de la Versión 4 de los que depende el software de Sun Cluster es opcional y se puede llevar a cabo como se describe en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#). (la actualización de los componentes compartidos de la Versión 2 a la Versión 5 es obligatoria).

NOTA	Si los componentes compartidos de Java ES se han sincronizado en la Versión 5, entonces el software de Sun Cluster debe actualizarse a la Versión 5. Esto es debido a que la Versión 4 de Sun Cluster no es compatible con el componente compartido Sun Java Web Console de la Versión 5.
-------------	---

Si se ha actualizado Sun Java Web Console a la Versión 5 (Ver 3.0), entonces tiene que aplicar las últimas revisiones de Sun Cluster o actualizar Sun Cluster, tal y como se describe en este capítulo.

Obtenga las contraseñas y la información de configuración necesarias

No es necesaria ninguna información especial sobre la versión instalada actualmente. Sin embargo, deberá iniciar sesión como superusuario para realizar la actualización.

Actualización del software de Sun Cluster

En esta sección, se abordan diversas consideraciones que afectan al proceso de actualización del software de Sun Cluster, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de Sun Cluster a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Al actualizar el software de la estructura de Sun Cluster, es recomendable actualizar los servicios de datos necesarios para administrar los componentes de Java ES de alta disponibilidad o las demás aplicaciones que se ejecutan en el entorno del clúster.
- Al actualizar el software de Sun Cluster, se ofrece la oportunidad de actualizar los componentes de Java ES o el resto de aplicaciones que se ejecutan en el entorno del clúster.

Procedimiento de actualización

El procedimiento descrito a continuación hace referencia a la actualización del software de Sun Cluster en cada nodo del clúster. Los pasos que aparecen a continuación son de carácter general; para obtener información detallada sobre estos pasos, consulte el capítulo sobre actualización de la *Sun Cluster Installation Guide*, <http://docs.sun.com/doc/819-0420/6n2rlnncr?a=view>. Las modificaciones para la Versión 5 de Sun Cluster se describen en *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>.

1. Inicie en modo sin clúster.
2. Inicie sesión como root o conviértase en superusuario.
su -
3. Acceda al siguiente directorio en la distribución de Java ES Versión 5:

```
cd /os_arch/Product/sun_cluster/os-ver/Tools
```

donde *os_arch* coincide con la plataforma, como, por ejemplo, *Solaris_sparc* y *os-ver* es *Solaris 9* o *Solaris 10*.

4. Ejecute la utilidad `scinstall`.

```
./scinstall
```

Aparecerá un menú principal para realizar las tareas de instalación, configuración y actualización del clúster.

5. Actualice el software de la estructura de Sun Cluster y los servicios de datos que desee.

Los servicios de datos actualizados deben configurarse mediante la migración de los recursos correspondientes a los tipos de recursos actualizados (consulte “Tareas posteriores a la actualización” en la página 92).

6. Aplique las revisiones necesarias al software de la estructura de Sun Cluster y a los servicios de datos.

Puede encontrar información sobre cómo acceder a las revisiones pertinentes y aplicarlas en el *Sun Cluster 3.0-3.1 Release Notes Supplement*, <http://docs.sun.com/app/docs/doc/816-3381/6m9lratq9?a=view#gcpom>.

7. Reinicie el nodo en el clúster.

Verificación de la actualización

Puede verificar si se ha realizado con éxito la actualización del software de Sun Cluster de la siguiente manera:

1. Introduzca el siguiente comando:

```
scinstall -pv
```

El comando devuelve la versión del software de Sun Cluster y de cada paquete de software instalado. Si este comando devuelve la versión 3.1 8/05, 3.1u4, entonces compruebe los números de revisiones para ver si tiene instalado el software de la Versión 4 o de la Versión 5, como se indica en la [Tabla 3-3 en la página 89](#).

2. Consulte el archivo de registro de actualización de los servicios de datos.

Se hace referencia a este archivo de registro al final de los mensajes de salida de la actualización.

Tareas posteriores a la actualización

Después de realizar la actualización del software de Sun Cluster, es posible que deba realizar una serie de tareas adicionales en función del tipo de actualización: conjunta o por turnos. Entre las tareas necesarias para restaurar por completo el entorno del clúster, se incluyen:

- Verificación del estado de la configuración del clúster
- Migración de los recursos a las nuevas versiones de tipos de recursos
- Actualización de los componentes de Java ES adicionales o las aplicaciones instaladas en el clúster

Para obtener información detallada sobre las tareas posteriores a la actualización, consulte el capítulo sobre actualización de la *Sun Cluster Installation Guide*, <http://docs.sun.com/doc/819-0420/6n2r1nncr?a=view>.

Anulación de la actualización

No se puede deshacer la actualización del software de Sun Cluster. Los cambios realizados durante el proceso de actualización no se pueden deshacer fácilmente.

Sun Cluster Geographic Edition

En este capítulo, se describe cómo actualizar Sun Cluster Geographic Edition a Java ES 5 (Versión 5): Sun Cluster Geographic Edition 3.1 2006Q4.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de las actualizaciones de Sun Cluster Geographic Edition” en la página 96
- “Actualización de Sun Cluster Geographic Edition desde la Versión 3.1 8/05” en la página 98

NOTA	Las ubicaciones de los archivos en este capítulo se especifican en relación con la ruta de directorio a la que se denomina <i>SunClusterGeo-base</i> . Debe haberse especificado, al menos, parte de esta ruta como directorio de instalación durante la instalación de Sun Cluster Geographic Edition. De lo contrario, el programa de instalación de Geographic Edition asigna un valor predeterminado. Los valores predeterminados de esta ruta de directorio se muestran en la siguiente tabla.
-------------	--

Tabla 4-1 Sun Cluster Geographic Edition Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>SunClusterGeo-base</i>	/opt/SUNWscgeo	No aplicable

Visión general de las actualizaciones de Sun Cluster Geographic Edition

En esta sección se describen los siguientes aspectos generales de Sun Cluster Geographic Edition que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Java ES Versión 5](#)
- [Guía de actualización deJava ES Versión 5](#)
- [Datos de Sun Cluster Geographic Edition](#)
- [Estrategia de actualización de Sun Cluster Geographic Edition](#)

Acerca de Java ES Versión 5

Java ES La Versión 5 de Sun Cluster Geographic Edition es la primera versión disponible de este producto como componente de Java ES; Sun Cluster Geographic Edition 3.1 se lanzó al principio como producto independiente.

La Versión 5 de Sun Cluster Geographic Edition representa una versión inferior en relación con Sun Cluster Geographic Edition 3.1 8/05. Es la primera versión disponible para la plataforma Solaris x86. La Versión 5 de Sun Cluster Geographic Edition también incluye soluciones determinadas de errores, calificaciones de varios componentes de hardware y software y compatibilidad con productos adicionales de repetición de datos.

Guía de actualización deJava ES Versión 5

La [Tabla 4-2](#) muestra las rutas de actualización compatibles de Sun Cluster Geographic Edition para Java ES Versión 5. Esta tabla sólo hace referencia al sistema operativo Solaris.

Tabla 4-2 Rutas de actualización a Java ES 5 (Versión 5): Sun Cluster Geographic Edition 3.1 2006Q4

Versión de Java ES	Sun Cluster Geographic Edition Versión	Enfoque general	Reconfiguración necesaria
Versiones anteriores de Java ES	Sun Cluster Geographic Edition 3.1 8/05	Actualización directa: Sustituya Sun Cluster Geographic Edition 3.1 8/05 mediante una instalación nueva	Ninguna

Datos de Sun Cluster Geographic Edition

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Sun Cluster Geographic Edition.

Tabla 4-3 Uso de datos de Sun Cluster Geographic Edition

Tipo de datos	Ubicación	Uso
Datos de configuración de Sun Cluster Geographic Edition	El depósito de configuración del clúster, que se replica y sincroniza en todos los nodos del clúster. (ADVERTENCIA: no edite nunca manualmente los archivos CCR, ya que un nodo o todo el clúster podría dejar de funcionar.)	Almacena información de configuración sobre todos los aspectos relacionados con las operaciones de Sun Cluster Geographic Edition.

Estrategia de actualización de Sun Cluster Geographic Edition

La estrategia utilizada para la actualización de Sun Cluster Geographic Edition depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Sun Cluster Geographic Edition presentando una serie de problemas que pueden influir en el plan de actualización de Sun Cluster Geographic Edition.

Problemas de compatibilidad

Los dos clústeres asociados tienen que ejecutar la misma versión de Sun Cluster Geographic Edition. Por lo tanto, la Versión 5 de Sun Cluster Geographic Edition no se puede combinar en asociación con Sun Cluster Geographic Edition 3.1 8/05 (no hay compatibilidad). La Versión 5 de Sun Cluster Geographic Edition incluye datos de configuración adicionales que no puede leer Sun Cluster Geographic Edition 3.1 8/05.

Dependencias

Las dependencias de Sun Cluster Geographic Edition con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Sun Cluster Geographic Edition. Por ejemplo, los cambios en las interfaces o las funciones de Sun Cluster Geographic Edition pueden requerir las versiones actualizadas de los componentes de los que depende Sun Cluster Geographic Edition. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Sun Cluster Geographic Edition presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Sun Cluster Geographic Edition presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Sun Cluster.** Sun Cluster Geographic Edition tiene una relación de dependencia obligatoria con Sun Cluster, que proporciona funciones de base.

Actualización de Sun Cluster Geographic Edition desde la Versión 3.1 8/05

En esta sección se incluye información sobre la actualización de Sun Cluster Geographic Edition de la Versión 3.1 8/05 a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Version 3.1 8/05 de Sun Cluster Geographic Edition](#)

Introducción

Al actualizar Sun Cluster Geographic Edition 3.1 8/05 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** La actualización se consigue mediante la desinstalación de la Versión 3.1 8/05 y una instalación nueva de la Versión 5 de Sun Cluster Geographic Edition. Se conservan los datos de configuración.

- **Dependencias de actualización.** Sun Cluster Geographic Edition presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realice una actualización de Sun Cluster Geographic Edition. En particular, Sun Cluster Geographic Edition tiene una fuerte relación de dependencia con el contenedor de agentes común, la versión 1.1. de Sun Cluster Geographic Edition y con Sun Cluster: La Versión 4 de Sun Cluster (3.1 8/05) debe actualizarse a la Versión 5 para que sea compatible con la Versión 5 de Sun Cluster Geographic Edition.
- **Compatibilidad con versiones anteriores.** La Versión 5 de Sun Cluster Geographic Edition no es compatible con Sun Cluster Geographic Edition 3.1 8/05. Todos los clústeres asociados deben actualizarse a la Versión 5.
- **Anulación de la actualización.** No se puede deshacer la actualización del software de Sun Cluster Geographic Edition a la Versión 3.1 8/05.
- **Problemas de plataforma.** El enfoque de actualización del software de Sun Cluster Geographic Edition es igual en todas las plataformas Solaris y arquitecturas de hardware. Sin embargo, no se admite el software de Sun Cluster Geographic Edition en las plataformas Linux.

Actualización de la Version 3.1 8/05 de Sun Cluster Geographic Edition

En esta sección se describe cómo realizar una actualización de la versión 3.1 8/05 de Sun Cluster Geographic Edition a Java ES Versión 5. En esta sección se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 3.1 8/05 de Sun Cluster Geographic Edition](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Sun Cluster Geographic Edition, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Prepare un clúster para la actualización](#)
- [Actualización de las dependencias de Sun Cluster Geographic Edition](#)
- [Copia de seguridad de los datos de Sun Cluster Geographic Edition](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Sun Cluster Geographic Edition, utilice el siguiente comando:

```
/usr/cluster/bin/geoadm --version
```

La cadena de la versión está situada después del texto de copyright y se muestra en la siguiente tabla:

Tabla 4-4 Resultados de la verificación de la versión de Sun Cluster Geographic Edition	
Versión de Java ES	Número de versión de Sun Cluster Geographic Edition
Versión 3.1 8/05	1.0
Componente de producto de la	1.1

Prepare un clúster para la actualización

Realice los siguientes pasos en todos los clústeres que estén asociados con el clúster que esté actualizando. El procedimiento elimina la capa de Sun Cluster Geographic Edition de la producción.

1. Asegúrese de que el clúster funciona correctamente.

Para ver el estado actual del clúster, ejecute el siguiente comando desde cualquier nodo.

scstat
2. Inicie sesión como root o conviértase en superusuario.

su -

3. Elimine todos los grupos de recursos de las aplicaciones de los grupos de protección.

Las aplicaciones de alta disponibilidad no tienen tiempo de inactividad durante la instalación de Sun Cluster Geographic Edition.

```
geopg remove-resource-group resourcegroup protectiongroupname
```

4. Lleve a cabo del [Paso 1](#) al [Paso 3](#) en todos los clústeres asociados con éste.
5. Detenga todos los grupos de protección activos en el clúster.

```
geopg stop protectiongroupname -e local | global
```

6. Elimine el complemento ICRM de todos los latidos en los dos clústeres asociados.

```
geohp remove-plugin icrmpugin heartbeatname
```

Actualización de las dependencias de Sun Cluster Geographic Edition

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Sun Cluster Geographic Edition presenta fuertes relaciones de dependencia con varios componentes compartidos y con Sun Cluster.

Al actualizar las dependencias de Sun Cluster Geographic Edition, debe seguir el orden que le mostramos a continuación (omitiendo cualquiera que ya se haya actualizado), antes de actualizar Sun Cluster Geographic Edition. Normalmente, el programa de instalación de Java ES realiza automáticamente la actualización de los componentes compartidos.

1. **Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Sun Cluster Geographic Edition cuando realiza una actualización a la Versión 5 de Sun Cluster Geographic Edition.

NOTA

Si se actualizan los componentes compartidos a la Versión 5 de Java ES, entonces debe actualizarse también el software de Sun Cluster Geographic Edition a la Versión 5. Esto es así porque Sun Cluster Geographic Edition 3.1 8/05 no es compatible con la Versión 5 de Sun Java Web Console.

- 2. Sun Cluster.** Las instrucciones para actualizar Sun Cluster a la Versión 5 están disponibles en el [Capítulo 3, “Software de Sun Cluster” en la página 81.](#)

Copia de seguridad de los datos de Sun Cluster Geographic Edition

Sun Cluster Geographic Edition almacena todos los datos en el depósito de configuración del clúster, por lo que no es necesario realizar una copia de seguridad de los datos actuales.

Obtenga las contraseñas y la información de configuración necesarias

No es necesaria ninguna información especial sobre la versión instalada actualmente. Sin embargo, deberá iniciar sesión como superusuario para realizar la actualización.

Actualización de la Versión 3.1 8/05 de Sun Cluster Geographic Edition

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Sun Cluster Geographic Edition, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

La actualización del software de Sun Cluster Geographic Edition a Java ES Versión 5 puede realizarse sin alterar las aplicaciones que se estén ejecutando. Puede actualizar el software de Sun Cluster Geographic Edition en un clúster que se esté ejecutando sin alteración, el clúster permanece en producción con todos los servicios que se estén ejecutando. De forma similar puede aplicar revisiones de Sun Cluster Geographic Edition sin tiempo de inactividad. Los datos de configuración se conservan en todo el proceso de actualización.

El software de Sun Cluster Geographic Edition debe actualizarse en todos los nodos de todos los clústeres que estén asociados con el clúster que está actualizando.

Si quiere que se actualice el sistema operativo Solaris durante el proceso de actualización del software de Sun Cluster Geographic Edition, debe eliminar los paquetes de Sun Cluster Geographic Edition antes de actualizar el sistema operativo Solaris.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia a las instancias de Sun Cluster Geographic Edition que residen localmente en el equipo en el que se vaya a realizar la actualización.

1. Inicie la sesión como root o conviértase en superusuario.

```
su -
```

2. Cierre Sun Cluster Geographic Edition 3.1 8/05.

```
/usr/cluster/bin/geoadm stop
```

Si quiere que se sigan ejecutando las aplicaciones subyacentes mientras se cierra Sun Cluster Geographic Edition, consulte la Sun Cluster Geographic Edition *Administration Guide*, <http://docs.sun.com/doc/817-7501>.

3. Desinstale Sun Cluster Geographic Edition 3.1 8/05.

```
SunClusterGeo-base/install/uninstall/uninstaller
```

Utilice el programa de instalación de Sun Cluster Geographic Edition en el modo desinstalación, como se describe en la Sun Cluster Geographic Edition *Installation Guide*, <http://docs.sun.com/doc/817-7500>.

4. Si no se está ejecutando Sun Cluster, inícielo.

Sun Cluster debe estar ejecutándose para instalar Sun Cluster Geographic Edition. Puede comprobarlo con el comando `scstat`.

5. Realice una nueva instalación de la Versión 5 de Sun Cluster Geographic Edition mediante el programa de instalación de Java ES.

- a. Inicie el programa de instalación de Java ES en el equipo que aloje la Versión 4 de Access Manager.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, `Solaris_sparc`. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b. Seleccione Sun Cluster Geographic Edition en la página de selección de componentes.

- c. Seleccione Configurar ahora o Configurar más tarde.
Puede seleccionar cualquiera de estas opciones porque no se necesita reconfiguración.
- d. Si fuera necesario, seleccione la opción para instalar paquetes traducidos.
- e. Una vez completada la instalación, salga del programa de instalación de Java ES.

NOTA Si está actualizando el software de Sun Cluster Geographic Edition en el SO Solaris 8, debe utilizar el comando `pkgadd` para instalar el software desde la distribución de la Versión 5 de Java ES. El programa de instalación de Java ES no admite la instalación del software de Sun Cluster Geographic Edition en SO Solaris 8.

- 6. Instale todas las revisiones necesarias de Sun Cluster Geographic Edition.

Para más instrucciones, consulte la *Sun Cluster Geographic Edition Installation Guide*, <http://docs.sun.com/doc/817-7500>.

- 7. Lleve a cabo del [Paso 1 en la página 103](#) al [Paso 6](#) en todos los clústeres asociados con éste.

- 8. Reinicie el software de la Versión 5 de Sun Cluster Geographic Edition.

```
/usr/cluster/bin/geoadm start
```

Si el clúster está en asociación, todos los nodos de los dos socios deben actualizarse antes de que se inicie el software de Sun Cluster Geographic Edition.

Para más información, consulte la *Installation Guide* mencionada anteriormente y la *Sun Cluster Geographic Edition Administration Guide*, <http://docs.sun.com/doc/817-7501>.

- 9. Añada todos los grupos de recursos de las aplicaciones que había eliminado cuando estaba preparando el clúster para la actualización, como se describe en [“Prepare un clúster para la actualización” en la página 100](#).

```
geopg add-resource-group resourcegroup protectiongroupname
```

- 10. Inicie todos los grupos de protección que ha añadido.

```
geopg start protectiongroupname -e local | global [-n]
```

Verificación de la actualización

Puede verificar si se ha realizado con éxito la actualización del software de Sun Cluster Geographic Edition de la siguiente manera:

1. Ejecute el siguiente comando:

```
/usr/cluster/bin/geoadm --version
```

Consulte la [Tabla 4-4 en la página 100](#) para obtener los valores de salida.

2. Si fuera necesario, después de haber actualizado los dos socios, ejecute los siguientes comandos en el nodo del clúster de cada socio.

```
/usr/cluster/bin/geoadm start
/usr/cluster/bin/geoadm show
```

El comando mostrará si el software de Sun Cluster Geographic Edition está activo en ese nodo.

Tareas posteriores a la actualización

No hay tareas posteriores a la actualización, más allá de las descritas en [“Procedimiento de actualización” en la página 102](#).

Anulación de la actualización

No se puede deshacer la actualización del software de Sun Cluster Geographic Edition.

Sin embargo, puede eliminar la Versión 5 de Sun Cluster Geographic Edition mediante la función de desinstalación del programa de instalación de Java ES y, a continuación, utilizar el programa de instalación de la versión 3.1 8/05 para volver a instalar la versión 3.1 8/05, porque la Versión 5 de Sun Cluster Geographic Edition escribe datos que la versión 3.1 8/05 no puede leer. Dicha anulación tiene que realizarse antes de iniciar la Versión 5, es decir, antes de que empiece a actualizar el software de Sun Cluster Geographic Edition, como se describe en el [“Procedimiento de actualización” en la página 102](#).

Directory Server

En este capítulo se describe cómo actualizar Directory Server a Java ES 5 (Versión 5): Sun Java System Directory Server 6.0.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Directory Server” en la página 109
- “Actualización de Directory Server desde Java ES Versión 4” en la página 114
- “Actualización de Directory Server desde Java ES Versión 3” en la página 123
- “Actualización de Directory Server desde Java ES Versión 2” en la página 123

NOTA Las ubicaciones de los archivos de este capítulo se especifican en relación con las rutas de directorio a las que se denomina *serverRoot* (Directory Server 5.x) y *DirServer-base* (Directory Server 6.0). Debe haberse especificado, al menos, una parte de estas rutas como directorios de instalación durante la instalación de Directory Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado.

Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.

Tabla 5-1 Directory Server Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>serverRoot</i> (Directory Server 5.x)	/var/opt/mps/serverroot	/var/opt/sun/directory-server
<i>DirServer-base</i> (Directory Server 6.0)	/opt/SUNWdsee	/opt/sun

Visión general de la actualización de Directory Server

En esta sección se describen los siguientes aspectos generales de Directory Server que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Java ES Versión 5](#)
- [Guía de actualización de Java ES Versión 5](#)
- [Datos de Directory Server](#)
- [Estrategia de actualización para Directory Server](#)

Acerca de Java ES Versión 5

Java ES La Versión 5 de Directory Server representa una versión superior con una variedad de nuevas funciones y mejoras. Para obtener más información, consulte *Directory Server Enterprise Edition 6 Release Notes*, <http://docs.sun.com/doc/819-0991>.

Guía de actualización de Java ES Versión 5

La [Tabla 5-2](#) muestra las rutas de actualización compatibles de Directory Server para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 5-2 Rutas de actualización a Java ES 5 (Versión 5): Directory Server 6.0

Versión de Java ES	Directory Server Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Directory Server 5.2 2005Q4	Actualización directa: Nueva instalación y migración de todos los datos.	Datos de configuración migrados desde una versión anterior a una nueva instalada en Directory Server
	Sun Java System Administration Server 5.2 2005Q4	Función de Administration Server sustituida por el centro de control del servicio de directorios y las utilidades de línea de comandos de Directory Server EE.	

Tabla 5-2 Rutas de actualización a Java ES 5 (Versión 5): Directory Server 6.0

Versión de Java ES	Directory Server Versión	Enfoque general	Reconfiguración necesaria
Versión 3	Sun Java System Directory Server 5 2005Q1	Actualización directa: Nueva instalación y migración de todos los datos.	Datos de configuración migrados desde una versión anterior a una nueva instalada en Directory Server
	Sun Java System Administration Server 5 2005Q1	Función de Administration Server sustituida por el centro de control del servicio de directorios y las utilidades de línea de comandos de Directory Server EE.	
Versión 2	Sun Java System Directory Server 5.2 2004Q2	Actualización directa: Nueva instalación y migración de todos los datos.	Datos de configuración migrados desde una versión anterior a una nueva instalada en Directory Server
	Sun Java System Administration Server 5.2 2004Q2	Función de Administration Server sustituida por el centro de control del servicio de directorios y las utilidades de línea de comandos de Directory Server EE.	
Versión 1	Sun ONE Directory Server 5.2	Actualización directa no certificada: Aunque puede utilizar el mismo enfoque que el de la actualización desde la Versión 2.	Datos de configuración migrados desde una versión anterior a una nueva instalada en Directory Server
	Sun ONE Administration Server 5.2		
Versiones anteriores de Java ES	Sun ONE Directory Server 5.2	Actualización directa no certificada: Aunque puede utilizar el mismo enfoque que el de la actualización desde la Versión 2.	Datos de configuración migrados desde una versión anterior a una nueva instalada en Directory Server
	Sun ONE Administration Server 5.2		
	Sun ONE Directory Server 5.1 Sun ONE Administration Server 5.1	Sin actualización directa: Actualice primero a la Versión 3. Consulte la <i>Guía de migración y actualización de Java Enterprise System 2005Q1</i> , http://docs.sun.com/doc/819-0062 . A continuación, actualice de la Versión 3 a la Versión 5.	Consulte la <i>Guía de migración y actualización de Java Enterprise System 2005Q1</i> , http://docs.sun.com/doc/819-0062 .

Datos de Directory Server

Directory Server 5.Las versiones de x utilizaban Directory Server para el almacenamiento de datos de configuración. Los datos se almacenaban en una estructura de árbol específica dentro del directorio. La instancia de Directory Server que aloja la configuración se denominaba directorio de configuración. Este directorio podía residir en el mismo equipo que otras instancias de Directory Server. Sin embargo, en la mayoría de las arquitecturas de implementación, el directorio de configuración estaba ubicado de forma remota en relación con los demás componentes, que lo utilizan para almacenar información de configuración.

Directory Server 6.0 ya no almacena datos de configuración en un directorio de configuración. La configuración se lleva a cabo mediante el centro de control del servicio de directorios (o las utilidades de línea de comandos de Directory Server EE) y tiene que accederse a ella mediante esta interfaz. El centro de control del servicio de directorios almacena datos de configuración en su propia instancia local de Directory Server.

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Directory Server a la Versión 5.

Tabla 5-3 Uso de datos de Directory Server

Tipo de datos	Ubicación	Uso
Datos de configuración de Directory Server	Directory Server 5.1 y 5.2: directorio de configuración Directory Server 6.0: al que se accede mediante el centro de control del servicio de directorios y de las utilidades de línea de comandos de Directory Server EE	Configuración de instancias de Directory Server
Esquema de Directory Server		Definición de estructura y semántica de datos en el directorio
Datos de seguridad	Directory Server 5.1 y 5.2: SSL configurado mediante la consola de Directory Server. Directory Server 6.0: SSL configurado mediante el centro de control del servicio de directorios y las utilidades de línea de comandos de Directory Server EE.	Certificados del servidor.
Datos de usuario	Directory Server	Admite aplicaciones con datos de configuración específicos del usuario y con perfiles de usuario.

Estrategia de actualización para Directory Server

La estrategia utilizada para la actualización de Directory Server depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Directory Server presentando una serie de problemas que pueden influir en el plan de actualización de Directory Server.

Problemas de compatibilidad

No se han introducido cambios en la interfaz de Directory Server de Java ES Versión 5 y es, por lo tanto, compatible con versiones anteriores. Además es compatible con todos los componentes admitidos por la Versión 4 de Directory Server y por versiones anteriores.

Sin embargo, la Versión 5 introduce cambios en las interfaces administrativas privadas. Las interfaces de la Versión 5 son incompatibles con versiones anteriores de Directory Server. Administration Server en particular, que solía configurar instancias anteriores de Directory Server, ha sido reemplazado por el centro de control de servicios de directorios y por las utilidades de línea de comandos de Directory Server, y ha sido eliminado el sufijo de directorio `o=NetscapeRoot`, que servía para almacenar información de configuración de Directory Server. Para más información, consulte la *Directory Server Enterprise Edition 6 Migration Guide*, <http://docs.sun.com/doc/819-0994>.

Dependencias

En general, las dependencias respecto de otros componentes de Java ES pueden afectar al procedimiento de actualización del software de Directory Server.

Directory Server presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Directory Server presenta relaciones de dependencia con componentes compartidos específicos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). La actualización de Directory Server puede depender de las versiones actualizadas de estos componentes compartidos.

- **Directory Proxy Server.** Directory Server tiene una dependencia conjunta con Web Proxy Server para proporcionar seguridad y rendimiento mejorados a las solicitudes LDPA.

Actualización de Directory Server desde Java ES Versión 4

En esta sección se incluye información sobre la actualización de Directory Server desde Java ES 2005 Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Directory Server](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Directory Server de la Versión 4 a la Versión 5 de Java ES, hay que tener en cuenta los siguientes aspectos del proceso de actualización:

- **Enfoque general de actualización.** La actualización se consigue realizando una nueva instalación de la Versión 5 de Directory Server y, a continuación, utilizando las herramientas de migración para volver a crear las instancias anteriores de Directory Server en instancias nuevas y diferenciadas de la Versión 5 de Directory Server.
- **Dependencias de actualización.** Directory Server presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realice una actualización de Directory Server.
- **Compatibilidad con versiones anteriores.** La Versión 5 de Directory Server no es compatible con la Versión 4, tal y como se describe en [“Problemas de compatibilidad” en la página 112](#). Sin embargo, las herramientas de migración permiten que se migre el sufijo o=NescapeRoot si continúa manteniendo un conjunto de instancias de Directory Server que dependan de la estructura administrativa de Directory Server 5.x.
- **Anulación de la actualización.** Para deshacer la actualización a la Versión 5 se debe eliminar la versión anterior, que se mantiene intacta al actualizar a la Versión 5.
- **Problemas de plataforma.** El enfoque general de actualización de Directory Server es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de Directory Server

En esta sección se describe cómo realizar una actualización de Directory Server de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Directory Server](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Directory Server, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Directory Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)
- [Cree una imagen de Directory Server \(opcional\)](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Directory Server, reinicie el daemon de Directory Server con la opción -v:

```
cd serverRoot/bin/slapd/server
./ns-slapd -v
```

Tabla 5-4 Resultados de la verificación de la versión de Directory Server

Versión de Java ES	Número de versión de Directory Server
Versión 2	Sun Java(TM) System Directory Server/5.2_Patch_2
Versión 3	Sun Java(TM) System Directory Server/5.2_Patch_3
Versión 4	Sun Java(TM) System Directory Server/5.2_Patch_4

Tabla 5-4 Resultados de la verificación de la versión de Directory Server

Versión de Java ES	Número de versión de Directory Server
Componente de producto de la	Sun Java(TM) System Directory Server/6.0

si falla el comando `ns-slapd` en la plataforma Solaris 10, establezca la ruta de biblioteca en "null" al ejecutar el comando:

```
LD_LIBRARY_PATH= ./ns-slapd -v
```

Actualización de las dependencias de Directory Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Sin embargo, todos los componentes compartidos que necesita Directory Server se actualizan automáticamente cuando se realiza la actualización de Directory Server a la Versión 5.

Obtenga las contraseñas y la información de configuración necesarias

Debe conocer el Id. de usuario y la contraseña del administrador de la versión de Directory Server actualmente instalada. Otra información de configuración se preserva durante el proceso de actualización.

Cree una imagen de Directory Server (opcional)

En los casos en los que la Versión 5 de Directory Server se instala en un equipo diferente del equipo en el que reside la Versión 4, debe crearse una imagen de la Versión 4 en el equipo en el que vaya a instalarse la Versión 5 de Directory Server. La imagen es necesaria para automatizar la migración de datos (mediante el comando `dsmig`) a las nuevas instancias de la Versión 5 de Directory Server.

La imagen de la Versión 4 incluye todos los archivos de esquema, de configuración, de seguridad y de bases de datos, con un diseño idéntico al de la estructura original de archivo de Directory Server 5.x *serverRoot*. La imagen es necesaria para llevar a cabo la migración de datos a las nuevas instancias de la Versión 5 de Directory Server.

Actualización de la Versión 4 de Directory Server

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Directory Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de Directory Server a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Cualquier componente de Java ES que utilice una instancia de Directory Server (como Access Manager o Portal Server, o los componentes de Sun Java Communications Suite) debe cerrarse y volverse a configurar, si fuera necesario, para acceder a la nueva instancia correspondiente de la Versión 5.
- En una arquitectura de implementación en la que haya varias instancias de Directory Server ejecutándose en un único equipo (todas correspondientes a la misma imagen instalada de Directory Server), sólo tiene que actualizar la imagen de Directory Server una vez. Sin embargo, deberá migrar los datos de cada una de las instancias por separado.
- En muchas arquitecturas de implementación de la Versión 4 de Directory Server, el directorio de configuración es una instancia diferente de Directory Server. Estas instancias no necesitan ser actualizadas porque el directorio de configuración ha sido rechazado por la Versión 5. Por otra parte, la actualización tiene que conllevar la implementación de la consola administrativa de la Versión 5 de Directory Server (el centro de control del servicio de directorios) en un equipo diferente del que utilice para administrar remotamente las instancias de Directory Server.
- Con Directory Server se proporciona una herramienta de línea de comandos que ayuda a automatizar la migración de los datos de esquema, de configuración, de seguridad y de usuario. Esta herramienta de migración permite una migración paso a paso de los diferentes tipos de datos. La mayoría de los escenarios se benefician de la migración automatizada de, al menos, algunos de los datos.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia a las instancias de Directory Server que residen localmente en el equipo en el que se vaya a realizar la actualización o, en el caso de que las instancias se vayan a mover a otro equipo, a todas las instancias que se vayan a ejecutar en el equipo de destino.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Cierre las instancias de la Versión 4 de Directory Server (5.2).

`serverRoot/slapd-instanceName/stop-slapd`

Compruebe que el registro de errores (`serverRoot/slapd-hostName/logs/errors`) proporciona un informe de cierre limpio:

```
[23/Jan/2006:15:56:47 +0100]: todos los subprocesos de la base de datos  
están detenidos
```

```
[23/Jan/2006:15:56:50 +0100]: slapd detenido.
```

3. Asegúrese de que el equipo host de la Versión 5 de Directory Server dispone de suficiente espacio en el disco.

El cálculo básico es el siguiente:

$2 * (\text{espacio para el servidor existente}) + (\text{espacio para los archivos LDIF})$

Por desgracia, no hay ninguna herramienta que permita anticipar el tamaño de un archivo LDIF creado a partir de una base de datos exportada. El tamaño dependerá del número de entradas de datos, de su representación interna, del número de índices, etc.

4. Para instalar remotamente la Versión 5, cree una imagen de la Versión 4 y transfírala al equipo remoto.

Consulte el [“Cree una imagen de Directory Server \(opcional\)” en la página 116](#).

5. Asegúrese de que ha actualizado todos los componentes de Java ES con los que Directory Server tiene una fuerte relación de dependencia (consulte [“Actualización de las dependencias de Directory Server” en la página 116](#)).

6. Realice una nueva instalación de la Versión 5 de Directory Server.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES.

```
cd java ES Release 5 distribution/os_arch

./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b.** Seleccione el subcomponente de Directory Server de Directory Server Enterprise Edition.

Tendrá que instalar también los subcomponentes administrativos (panel de control del servicio de directorios o utilidades de línea de comandos) que desee utilizar.

- c.** Especifique una ruta de instalación diferente de cualquiera existente en la Versión 4 de Directory Server.
- d.** Seleccione Configurar ahora o Configurar más tarde.

No importa qué opción elija, dado que Directory Server no precisa de configuración alguna. Sin embargo, si elije Configurar ahora, *no* opte por crear una nueva instancia.

- e.** Confirme las opciones de instalación seleccionadas.

Los paquetes de Directory Server se actualizarán y se mostrará un resumen de la actualización.

- f.** Salga del programa de instalación de Java ES.

7. Cree una instancia de Directory Server.

DirServer-base/ds6/bin/dsadm create instancePath

donde *instancePath* es la ruta completa a la instancia de Directory Server.

Para obtener información sobre cómo crear una instancia de Directory Server, consulte la *Directory Server Enterprise Edition 6 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

Si no consigue crear una nueva instancia, se creará una nueva automáticamente cuando se migren los datos con el comando *dsmig* ([Paso 8](#)).

Si falla el comando *dsadm* en la plataforma Solaris 10, establezca la ruta de biblioteca en “null” al ejecutar el comando:

LD_LIBRARY_PATH= ./dsadm create instancePath

8. Migre la instancia de Directory Server de la Versión 4 a la Versión 5.

Utilice los comandos *DirServer-base/ds6/bin/dsmig*.

Los comandos *dsmig* adaptan los datos de la Versión 4 al formato de la Versión 5 y los escriben en las ubicaciones adecuadas. Por ejemplo, la migración típica en un único equipo con una instancia de Directory Server debe tener el siguiente aspecto:

```
dsmig migrate-schema -v old_instancePath new_instancePath

dsmig migrate-config -v old_instancePath new_instancePath

dsmig migrate-security -v old_instancePath new_instancePath

dsmig migrate-data -v old_instancePath new_instancePath
```

NOTAS

- Si falla el comando `dsmig migrate-config` en la plataforma Solaris 10, establezca la ruta de biblioteca en “null” al ejecutar el comando:

```
LD_LIBRARY_PATH= ./dsmig migrate-config ...
```

- Si la instancia de Directory Server que se está migrando guarda datos de configuración de otros componentes de Java ES como, por ejemplo, el componente Messaging Server de Sun Java Communications Suite, tendrá que migrar una parte específica del árbol de información de directorio con el nombre `o=netscaperoot`. Este sufijo raíz no se migra de forma predeterminada. Para migrar `o=netscaperoot`, utilice la opción `-N` de `dsmig migrate-config` y los comandos `dsmig migrate-data`. Por ejemplo:

```
dsmig migrate-config -v old_instancePath
new_instancePath -N
```

- Si está migrando desde una instancia de una arquitectura de 32 bits a otra de 64 bits, no es posible utilizar el comando (herramienta de migración automática) `dsmig migrate-data`. Tiene que migrar los datos manualmente, como se describe en la *Guía de migración* a la que se hace referencia a continuación. No obstante, todavía puede realizar una migración automática de los datos de esquema, de configuración y de seguridad.
 - En algunos casos, cuando se inicia Directory Server después de que se hayan migrado los datos de directorio, la nueva comprobación de errores de la Versión 5 detecta definiciones circulares en las entradas de grupo de Directory Server. Estas definiciones circulares son funcionalmente benignas, pero pueden provocar un gran número de errores que pueden quedar registrados en el archivo de errores.
-

Para más detalles sobre el proceso de migración, los comandos `dsmig` y la migración manual, consulte la *Directory Server Enterprise Edition 6 Migration Guide*, <http://docs.sun.com/doc/819-0994>.

Verificación de la actualización

Puede verificar si se ha realizado con éxito la actualización de Directory Server de la siguiente manera:

1. Inicie la nueva instancia de Directory Server:

DirServer-base/ds6/bin/dsadm -V

Consulte la [Tabla 5-4 en la página 115](#) para obtener los valores de salida.

2. Compruebe los mensajes de inicio en el registro de errores de Directory Server:

instancePath/logs/errors

NOTA	Al iniciarse, la Versión 5 de Directory Server detecta las definiciones circulares. Estas definiciones circulares son funcionalmente benignas, pero pueden provocar un gran número de errores si va a actualizar desde una versión anterior que contiene dichas definiciones circulares.
-------------	--

Tareas posteriores a la actualización

No hay tareas posteriores a la actualización, aparte de las descritas en [“Procedimiento de actualización” en la página 117](#), excepto que todos los componentes de Java ES que dependen de Directory Server deben volver a configurarse para que señalen a las nuevas instancias de Directory Server.

Anulación de la actualización

Para deshacer la actualización a la Versión 5 se debe eliminar la versión anterior, que se mantiene intacta al actualizar a la Versión 5.

Actualización de varias instancias

Los procedimientos descritos en [“Actualización de la Versión 4 de Directory Server” en la página 115](#) no abordan de forma explícita las arquitecturas de implementación en las que Directory Server se replica para obtener disponibilidad o escalabilidad. Entre estas arquitecturas se incluye la repetición de Directory Server o la implementación de Directory Server como servicio de datos en un entorno de Sun Cluster.

En esta sección se describen los procedimientos de actualización de Directory Server en estas situaciones.

Actualización por turnos de réplicas de Directory Server

Se pueden actualizar de forma secuencial (una instancia cada vez) varias instancias de Directory Server en diferentes sistemas informáticos, del mismo modo que en las arquitecturas de implementación de repetición de réplicas principales. Después de la primera sincronización de todas las réplicas de Directory Server, debe actualizar cada instancia en el equipo host respectivo mientras las demás instancias se dejan en ejecución. Esta actualización por turnos permite que el servicio de directorio permanezca en línea mientras se actualizan las instancias de Directory Server que proporcionan el servicio.

Actualización de Directory Server como servicio de datos

La información relativa a la actualización y la anulación de la actualización de Directory Server como servicio de datos en un entorno de Sun Cluster no está disponible todavía.

Actualización de Directory Server desde Java ES Versión 3

El procedimiento para actualizar Directory Server de Java ES 2003Q1 (Versión 3) a la Versión 5 es el mismo que el que se sigue para actualizar Directory Server de la Versión 4 a la Versión 5.

Para actualizar Directory Server de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Directory Server desde Java ES Versión 4” en la página 114](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Actualización de Directory Server desde Java ES Versión 2

El procedimiento para actualizar Directory Server de Java ES 2004Q2 (Versión 2) a la Versión 5 es el mismo que el procedimiento de actualización de Directory Server de la Versión 4 a la Versión 5, con la excepción de que las tareas previas a la actualización deben incluir la actualización de todos los componentes compartidos a la Versión 5 (consulte la [Tabla 1-7 en la página 49](#)).

Las instrucciones para actualizar los componentes compartidos de Java ES a la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).

Para actualizar Directory Server de la Versión 2 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Directory Server desde Java ES Versión 4” en la página 114](#) y sustituya la referencia a la Versión 4 por la Versión 2.

Directory Proxy Server

En este capítulo, se describe cómo actualizar Directory Proxy Server a Java ES 5 (Versión 5): Sun Java System Directory Proxy Server 6.0.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de las actualizaciones de Directory Proxy Server” en la página 127
- “Actualización de Directory Proxy Server desde Java ES Versión 4” en la página 132
- “Actualización de Directory Proxy Server desde Java ES Versión 3” en la página 139
- “Actualización de Directory Proxy Server desde Java ES Versión 2” en la página 140

NOTA Las ubicaciones de los archivos de este capítulo se especifican en relación con las rutas de directorio a las que se denomina *serverRoot* (Directory Proxy Server 5.x) y *DirServer-base* (Directory Proxy Server 6.0). Debe haberse especificado, al menos, una parte de estas rutas como directorios de instalación durante la instalación de Directory Proxy Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado.

Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.

Tabla 6-1 Directory Proxy Server Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>serverRoot</i> (Directory Proxy Server 5.x)	/var/opt/mps/serverroot	/var/opt/sun/directory-server
<i>DirServer-base</i> (Directory Proxy Server 6.0)	/opt/SUNWdsee	/opt/sun

Visión general de las actualizaciones de Directory Proxy Server

En esta sección se describen los siguientes aspectos generales de Directory Proxy Server que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Java ES Versión 5](#)
- [Guía de actualización de Java ES Versión 5](#)
- [Datos de Directory Proxy Server](#)
- [Estrategia de actualización para Directory Proxy Server](#)

Acerca de Java ES Versión 5

Directory Proxy Server de Java ES Versión 5 representa una versión superior y se puede considerar un nuevo producto en relación con la Versión 4 y todas las versiones anteriores de Directory Proxy Server.

La Versión 5 de Directory Proxy Server sigue siendo un proxy LDAP, pero con nuevas funciones de encaminamiento extensibles. La Versión 5 permite que con la función Directorio virtual se puedan agregar varios datos en una sola vista. Estas vistas de datos pueden representar almacenes de datos accesibles LDAP o SQL.

Para más información, consulte las *Directory Server Enterprise Edition 6 Release Notes*.

Guía de actualización de Java ES Versión 5

La [Tabla 6-2](#) muestra las rutas de actualización compatibles de Directory Proxy Server para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 6-2 Rutas de actualización a Java ES 5 (Versión 5): Directory Proxy Server 6.0

Versión de Java ES	Directory Proxy Server Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Directory Proxy Server 5.2 2005Q4	Actualización directa: Sustituya la Versión 4 con una nueva instalación y configuración de la Versión 5.	Si desea que sea compatible con las versiones anteriores, asigne manualmente la configuración anterior a las nuevas propiedades de configuración.
Versión 3	Sun Java System Directory Proxy Server 5.2 2005Q1	Actualización directa: Sustituya la Versión 3 con una nueva instalación y configuración de la Versión 5.	Si desea que sea compatible con las versiones anteriores, asigne manualmente la configuración anterior a las nuevas propiedades de configuración.
Versión 2	Sun Java System Directory Proxy Server 5.2 2004Q2	Actualización directa: Sustituya la Versión 2 con una nueva instalación y configuración de la Versión 5.	Si desea que sea compatible con las versiones anteriores, asigne manualmente la configuración anterior a las nuevas propiedades de configuración.
Versión 1	Sun ONE Directory Proxy Server 5.2	Actualización directa no certificada: Aunque puede utilizar el mismo enfoque que el de la actualización desde la Versión 2.	Si desea que sea compatible con las versiones anteriores, asigne manualmente la configuración anterior a las nuevas propiedades de configuración.
Versiones anteriores de Java ES	Sun ONE Directory Proxy Server 5.2	Actualización directa no certificada: Aunque puede utilizar el mismo enfoque que el de la actualización desde la Versión 2.	Si desea que sea compatible con las versiones anteriores, asigne manualmente la configuración anterior a las nuevas propiedades de configuración.
	Sun ONE Directory Access Router 5.0 ó 5.0 SP1	Sin actualización directa: Actualice primero a la Versión 3. Consulte la <i>Java Enterprise SystemGuía de migración y actualización de Java Enterprise System 2005Q1</i> , http://docs.sun.com/doc/819-0062 . A continuación, actualice de la Versión 3 a la Versión 5.	Consulte la <i>Java Enterprise SystemGuía de migración y actualización de Java Enterprise System 2005Q1</i> , http://docs.sun.com/doc/819-0062 .

Datos de Directory Proxy Server

Directory Proxy Server ya no utiliza Directory Server para el almacenamiento de los datos de configuración. La configuración se realiza mediante el nuevo centro de control del servicio de directorio o mediante las utilidades de línea de comandos de Directory Server EE.

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Directory Proxy Server.

Tabla 6-3 Uso de datos de Directory Proxy Server

Tipo de datos	Ubicación	Uso
Datos de configuración de Directory Proxy Server	Directory Proxy Server 5.2: directorio de configuración	Configuración de Directory Proxy Server
	Directory Proxy Server 6.0: al que se accede mediante el centro de control del servicio de directorio y las utilidades de línea de comandos de Directory Server EE.	
Datos de seguridad	Directory Proxy Server 5.2: SSL configurado mediante la consola de Directory Proxy Server.	Certificados del servidor
	Directory Proxy Server 6.0: SSL configurado mediante el centro de control del servicio de directorios y las utilidades de línea de comandos de Directory Server EE.	

Estrategia de actualización para Directory Proxy Server

La estrategia utilizada para la actualización de Directory Proxy Server depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Directory Proxy Server presentando una serie de problemas que pueden influir en el plan de actualización de Directory Proxy Server.

Problemas de compatibilidad

La Versión 5 de Directory Proxy Server introduce cambios en la interfaz que la hacen incompatible con versiones anteriores de Directory Proxy Server. La Versión 5 de Directory Proxy Server se fundamenta en una implementación totalmente nueva basada en Java y su configuración presenta importantes cambios en relación con la Versión 4 y las versiones anteriores de Directory Proxy Server.

Sin embargo, es posible configurar la Versión 5 de Directory Proxy Server para que sea compatible con versiones anteriores, es decir, para que funcione como la Versión 4 y las versiones anteriores de Directory Proxy Server. Esta configuración requiere la asignación manual de los atributos de la configuración anterior a las propiedades de configuración de la Versión 5. Para obtener más información, consulte la *Directory Server Enterprise Edition 6 Migration Guide*, <http://docs.sun.com/doc/819-0994>.

Sin embargo, la Versión 5 de Directory Proxy Server tiene funcionamientos predeterminados diferentes de los de versiones anteriores: no permite que los controles LDAP pasen por el proxy. Para reproducir el funcionamiento de versiones anteriores, puede desbloquear estos controles como se describe en “[Tareas posteriores a la actualización](#)” en la [página 137](#).

Dependencias

Las dependencias de otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Directory Proxy Server.

Directory Proxy Server presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Directory Proxy Server presenta relaciones de dependencia con componentes compartidos específicos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). La actualización de Directory Proxy Server puede depender de las versiones actualizadas de estos componentes compartidos.
- **Directory Server.** Directory Proxy Server tiene una codependencia con Directory Server para proporcionar seguridad y rendimiento mejorados a las solicitudes LDAP. Directory Proxy Server proporciona acceso en relación con la interfaz a Directory Server, pero no tiene dependencia de Directory Server aparte de esta relación funcional.

Actualización de Directory Proxy Server desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Directory Proxy Server desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Directory Proxy Server](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Directory Proxy Server de Java ES de la Versión 4 a la Versión 5, hay que tener en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** La actualización se consigue mediante una nueva instalación de la Versión 5 de Directory Proxy Server y una posterior configuración de las instancias nuevas de Directory Proxy Server mediante el centro de control del servicio de directorio o las utilidades de línea de comandos de Directory Server EE.
- **Dependencias de actualización.** Directory Proxy Server presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realice una actualización de Directory Proxy Server.
- **Compatibilidad con versiones anteriores.** La Versión 5 de Directory Proxy Server puede configurarse para que sea compatible con la Versión 4, como se explica en [“Problemas de compatibilidad” en la página 130](#).
- **Anulación de la actualización.** Para deshacer la actualización a la Versión 5 se debe eliminar la versión anterior, que se mantiene intacta al actualizar a la Versión 5.
- **Problemas de plataforma.** El enfoque general de actualización de Directory Proxy Server es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de Directory Proxy Server

En esta sección se describe cómo realizar una actualización de Directory Proxy Server de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Directory Proxy Server](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Directory Proxy Server, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Directory Proxy Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Directory Proxy Server, utilice los siguientes comandos:

```
cd serverRoot/bin/dps/server/bin
./ldapfwd -v
```

Los resultados se muestran en la siguiente tabla:

Tabla 6-4 Resultados de la verificación de la versión de Directory Proxy Server

Versión de Java ES	Número de versión de Directory Proxy Server
Versión 2	Sun ONE Directory Proxy Server Version 5.2_Patch_2
Versión 3	Sun ONE Directory Proxy Server Version 5.2_Patch_3
Versión 4	Sun ONE Directory Proxy Server Version 5.2_Patch_4

Tabla 6-4 Resultados de la verificación de la versión de Directory Proxy Server

Versión de Java ES	Número de versión de Directory Proxy Server
Versión 5 ¹	Sun ONE Directory Proxy Server Version 6.0

1. El comando `ldapfwd` no se puede utilizar para devolver un número de versión para la Versión 5. Consulte [“Verificación de la actualización” en la página 137](#).

Actualización de las dependencias de Directory Proxy Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Directory Proxy Server presenta fuertes relaciones de dependencia con sólo un par de componentes compartidos.

Al actualizar las dependencias de Directory Proxy Server, debe seguir el orden que le mostramos a continuación (omitiendo cualquiera que ya se haya actualizado), antes de actualizar Directory Proxy Server. Normalmente, el programa de instalación de Java ES realiza automáticamente la actualización de los componentes compartidos.

1. **Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Directory Proxy Server cuando realiza una actualización a la Versión 5 de Directory Proxy Server.
2. **Directory Server (dependencia leve de actualización).** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [Capítulo 5, “Directory Server” en la página 107](#). Sin embargo, la Versión 5 de Directory Proxy Server es compatible con la Versión 4 de Directory Server.

Obtenga las contraseñas y la información de configuración necesarias

La información de configuración se preserva durante el proceso de actualización y se puede utilizar para asignar los atributos de configuración de la Versión 5 a las propiedades de configuración de la Versión 5. Consulte el [“Problemas de compatibilidad” en la página 130](#).

Actualización de la Versión 4 de Directory Proxy Server

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Directory Proxy Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de Directory Proxy Server a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Se debe cerrar y reconfigurar cualquier componente de Java ES que utilice una instancia de Directory Proxy Server (como, por ejemplo, Access Manager, Communications Express, Messaging Server o Portal Server, entre otros) antes de acceder a la instancia nueva correspondiente de la Versión 5.
- En una arquitectura de implementación en la que haya varias instancias de Directory Proxy Server ejecutándose en un único equipo (todas correspondientes a la misma imagen instalada de Directory Proxy Server), al actualizar la imagen de Directory Proxy Server, tendrá que crear nuevas instancias de Directory Proxy Server.
- En las arquitecturas de implementación de la Versión 4 relacionadas con Directory Proxy Server, se ha utilizado un servidor de administración para configurar y administrar las instancias de Directory Proxy Server. En la Versión 5, la actualización de Directory Proxy Server debe conllevar la implementación del centro de control del servicio de directorio utilizado para configurar y administrar las instancias de Directory Proxy Server.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia a las instancias de Directory Proxy Server que residen localmente en el equipo en el que se vaya a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Cierre todos los componentes de Java ES que dependan de las instancias de Directory Proxy Server que se vayan a actualizar. Este paso puede depender de cómo se replique Directory Proxy Server en la arquitectura de implementación.

Para obtener información sobre cómo cerrar un componente de Java ES, consulte su guía de administración respectiva.

3. Realice una nueva instalación de la Versión 5 de Directory Proxy Server.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES.

```
cd Java ES Release 5 distribution/os_arch  
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”.)

- b. Seleccione el subcomponente de Directory Proxy Server de Directory Server Enterprise Edition.

Tendrá que instalar también los subcomponentes administrativos (panel de control del servicio de directorios o utilidades de línea de comandos) que desee utilizar.

- c. Especifique una ruta de instalación diferente de cualquiera existente en la Versión 4 de Directory Proxy Server.

- d. Seleccione Configurar ahora o Configurar más tarde.

No importa qué opción elija porque no es necesaria ninguna configuración para Directory Proxy Server. Sin embargo, si elige Configurar ahora, se le preguntará si quiere crear una instancia nueva. (Una vez que se haya instalado el componente, puede crear tantas instancias de Directory Proxy Server como desee.)

- e. Si fuera necesario, seleccione la opción para instalar paquetes traducidos.

- f. Confirme las opciones de instalación seleccionadas.

Los paquetes de Directory Proxy Server se instalarán y se mostrará un resumen de la instalación.

- g. Salga del programa de instalación de Java ES.

Si no ha creado una instancia nueva, continúe en el [Paso 4](#); de lo contrario, siga con el [Paso 5](#).

4. Cree una instancia de Directory Proxy Server.

DirServer-base/dps6/bin/dpadm create instancePath

donde *instancePath* es la ruta completa a la instancia de Directory Proxy Server.

Para obtener información sobre cómo crear una instancia de Directory Proxy Server, consulte la *Directory Server Enterprise Edition 6 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

5. Si lo desea, asigne los atributos de configuración de la Versión 4 a las propiedades de configuración de la Versión 5 de Directory Proxy Server.

Para más detalles sobre el proceso de asignación, consulte la *Directory Server Enterprise Edition 6 Migration Guide*, <http://docs.sun.com/doc/819-0994>.

Verificación de la actualización

Puede verificar si se ha realizado con éxito la actualización de Directory Proxy Server de la siguiente manera:

1. Inicie la nueva instancia de Directory Proxy Server:

DirServer-base/dps6/bin/dpadm start instancePath

2. Compruebe la versión de Directory Proxy Server.

DirServer-base/dps6/bin/dpadm --version

Los valores de salida se muestran en la [Tabla 6-4 en la página 133](#).

Tareas posteriores a la actualización

Todos los componentes de Java ES que dependan de Directory Proxy Server tienen que ser reconfigurados para que señalen a las instancias nuevas de Directory Proxy Server.

Además, para reproducir los funcionamientos predeterminados de versiones anteriores, debe permitirse explícitamente que los controles LDAP pasen por el proxy. Puede activar estos controles estableciendo la propiedad `allowed-ldap-controls` de la siguiente manera:

```
cd DirServer-base/dps6/bin
./dpconf set-server-prop
allowed-ldap-controls:auth-request
allowed-ldap-controls:chaining-loop-detection
allowed-ldap-controls:manage-dsa
allowed-ldap-controls:persistent-search
```

```
allowed-ldap-controls:proxy-auth-v1  
allowed-ldap-controls:proxy-auth-v2  
allowed-ldap-controls:real-attributes-only  
allowed-ldap-controls:server-side-sorting
```

Anulación de la actualización

Para deshacer la actualización a la Versión 5 se debe eliminar la versión anterior, que se mantiene intacta al actualizar a la Versión 5.

Actualización de varias instancias

En algunas arquitecturas de implementación, Directory Proxy Server se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que los componentes de Directory Proxy Server se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Si utiliza instancias de Directory Proxy Server con equilibrado de carga, no puede realizar una actualización por turnos; el equilibrador tiene que cerrarse y reconfigurarse para poder acceder a las instancias de la Versión 5. Debe realizar la actualización de cada instancia como se describe en [“Actualización de la Versión 4 de Directory Proxy Server” en la página 133](#).

Actualización de Directory Proxy Server desde Java ES Versión 3

El procedimiento para actualizar Directory Proxy Server de Java ES 2005Q1 (Versión 3) a la Versión 5 es el mismo que el que se sigue para actualizar Directory Proxy Server de la Versión 4 a la Versión 5.

Para actualizar Directory Proxy Server de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Directory Proxy Server desde Java ES Versión 4” en la página 132](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Actualización de Directory Proxy Server desde Java ES Versión 2

El procedimiento de actualización de Directory Proxy Server de Java ES 2004Q2 (Versión 2) a la Versión 5 es idéntico al procedimiento de actualización de Directory Proxy Server de la Versión 4 a la Versión 5, excepto que en las tareas previas a la actualización debe incluirse la sincronización en la Versión 5 de todos los componentes compartidos (consulte la [Tabla 1-7 en la página 49](#)) y todos los componentes de productos locales de los que dependa Directory Proxy Server.

Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).

Para actualizar Directory Proxy Server de la Versión 2 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Directory Proxy Server desde Java ES Versión 4” en la página 132](#) y sustituya la referencia a la Versión 4 por la Versión 2.

Web Server

En este capítulo, se describe cómo actualizar Web Server a Java ES 5 (Versión 5): Sun Java System Web Server 7.0.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Web Server” en la página 142
- “Actualización de Web Server desde Java ES Versión 4” en la página 146
- “Actualización de Web Server desde Java ES Versión 3” en la página 168
- “Actualización de Web Server desde Java ES Versión 2” en la página 169

NOTA Las ubicaciones de archivos incluidas en este capítulo se especifican en relación con las rutas de directorio a las que se hace referencia como *WebServer6-base* (Web Server 6.x) y *WebServer7-base* y *WebServer7Config-base* (Web Server 7.0). Debe haberse especificado, al menos, parte de estas rutas como directorio de instalación durante la instalación inicial de Web Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado.

Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.

Tabla 7-1 Web Server Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>WebServer6-base</i>	/opt/SUNWwbsvr	/opt/sun/webserver

Tabla 7-1 Web Server Rutas de directorio *(continúa)*

Variable de nombre de ruta	SO Solaris	SO Linux
<i>WebServer7-base</i>	/opt/SUNWwbsvr7	/opt/sun/webserver7
<i>WebServer7Config-base</i>	/var/opt/SUNWwbsvr7	/var/opt/sun/webserver7

Visión general de la actualización de Web Server

En esta sección se describen los siguientes aspectos generales de Web Server que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Web Server de Java ES Versión 5](#)
- [Guía de actualización de Web Server](#)
- [Datos de Web Server](#)
- [Estrategia de actualización para Web Server](#)

Acerca de Web Server de Java ES Versión 5

El componente Web Server de Java ES Versión 5 representa un avance importante en relación con la Versión 4, ya que incluye una serie de nuevas funciones y mejoras de la interfaz.

La Versión 5 de Web Server presenta una nueva infraestructura administrativa con nuevas herramientas de administración. La infraestructura administrativa incluye una instancia del servidor de administración que aloja la información de configuración de varias instancias de Web Server. La nueva interfaz de línea de comandos (*wadm*) y la nueva interfaz gráfica de usuario se utilizan para crear las instancias de Web Server, ya sea de forma local o en equipos remotos, y para configurar y administrar estas instancias. Las nuevas herramientas de administración requieren un nombre de usuario y una contraseña de administrador.

Para obtener más información sobre la nueva infraestructura administrativa, consulte *Web Server 7.0 Administrator's Guide*, <http://docs.sun.com/doc/819-2629>.

Estos cambios efectuados en la interfaz administrativa de Web Server afectan de forma significativa a la actualización.

Guía de actualización de Web Server

La [Tabla 7-2](#) muestra las rutas de actualización compatibles de Web Server para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 7-2 Rutas de actualización a Java ES 5 (Versión 5): Web Server 7.0

Versión de Java ES	Web Server Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Web Server 6.1 SP5 2005Q4	Actualización directa: nueva instalación, seguida de la migración de datos.	Migración de la configuración de instancias a las nuevas instancias.
Versión 3	Sun Java System Web Server 6 2005Q1 Update 1 SP 4	Actualización directa: nueva instalación, seguida de la migración de datos.	Migración de la configuración de instancias a las nuevas instancias.
Versión 2	Sun Java System Web Server 6 2004Q2 Update 1 SP 2 Platform Edition y Enterprise Edition	Actualización directa: nueva instalación, seguida de la migración de datos.	Migración de la configuración de instancias a las nuevas instancias.
Versión 1	Sun ONE Web Server 6.1 (2003Q4)	Actualización directa no certificada: aunque se puede realizar mediante una nueva instalación, seguida de la migración de datos.	Migración de la configuración de instancias a las nuevas instancias.
Versiones anteriores de Java ES		Sin actualización directa.	

Datos de Web Server

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Web Server.

Tabla 7-3 Uso de datos de Web Server

Tipo de datos	Ubicación	Uso
Datos de configuración	Web Server 6.x (Java ES Versión 2, 3 y 4): <i>WebServer6-base/https-instanceName/config/</i>	Configuración de instancias de Web Server
	Web Server 7.0 (Java ES Versión 5): Configuración de instancias <i>WebServer7Config-base/https-configName/config¹/</i>	
	Almacén de configuración central	
	Se accede a él mediante la consola de Web Server y la interfaz de línea de comandos wadm.	

1. Tenga en cuenta que la ruta de *WebServer7Config-base* es bastante diferente de la ruta de *WebServer6-base*.

Estrategia de actualización para Web Server

La estrategia utilizada para la actualización de Web Server depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Web Server presentando una serie de problemas que pueden influir en el plan de actualización de Web Server.

Problemas de compatibilidad

El componente Web Server de Java ES Versión 5 no presenta ningún cambio en las interfaces públicas por lo que, en este sentido, es compatible con versiones anteriores. Sin embargo, las nuevas interfaces administrativas no presentan compatibilidad con las interfaces administrativas de versiones anteriores. Esto afecta a la actualización y la reimplementación de las aplicaciones web (incluidos, por ejemplo, los componentes de Java ES).

En concreto, la Versión 5 de Web Server utiliza diferentes valores predeterminados para los directorios de instancias y los nombres de servidor virtual, como se muestra en la siguiente tabla.

Tabla 7-4 Nombres predeterminados de Web Server

Elemento	Valor predeterminado de Web Server 6.x de Java ES Versión 2, 3 y 4	Java ES Versión 5 Web Server 7.0 predeterminado
Nombre de configuración		<i>hostName.domainName</i>
Ruta del directorio de la instancia	<i>WebServer6-base/ https-hostName.domainName</i>	<i>WebServer7Config-base https-hostName.domainName</i>
Nombre del servidor virtual	<i>https-hostName.domainName</i>	<i>hostName.domainName</i>

Web Server Dependencias

Web Server presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Web Server presenta relaciones de dependencia con componentes compartidos específicos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Las actualizaciones de Web Server pueden depender de las versiones actualizadas de estos componentes compartidos.
- **Directory Server.** Web Server presenta una relación de dependencia opcional con Directory Server para proporcionar autenticación basada en LDAP.
- **Web Proxy Server.** Web Server presenta una relación de codependencia con Web Proxy Server para proporcionar mejoras en el rendimiento y la seguridad de las solicitudes HTTP.

Actualización de Web Server desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Web Server desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Web Server](#)

Introducción

Al actualizar Web Server de Java ES de la Versión 4 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque de actualización general.** La actualización se realiza mediante una nueva instalación de la Versión 5 de Web Server, la migración de la información de configuración de las instancias de la Versión 4 de Web Server a una configuración de la Versión 5 y la creación de las instancias de la Versión 5 de Web Server que se correspondan con las instancias de la Versión 4.
- **Dependencias de actualización.** Web Server presenta relaciones de dependencia con una serie de componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)); el programa de instalación de Java ES actualiza todos estos componentes compartidos a la Versión 5 al realizar una actualización de Web Server. Web Server presenta sólo fuertes relaciones de dependencia de actualización con los componentes compartidos NSS y NSPR.
- **Compatibilidad con versiones anteriores.** Las interfaces administrativas de la Versión 5 de Web Server no son compatibles con la Versión 4.
- **Anulación de la actualización.** Para anular la actualización a la Versión 5, es necesario restablecer la instalación de la Versión 4, que permanece intacta.
- **Problemas de plataforma.** El enfoque general de actualización de Web Server es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de Web Server

En esta sección se describe cómo realizar una actualización de Web Server de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Web Server](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Web Server, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Web Server](#)
- [Copia de seguridad de los datos de Web Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Puede verificar la versión actual de Web Server ejecutando el servidor de la instancia de Web Server con la opción `-version`:

```
WebServer6-base/https-hostName.domainName/start -version
```

Tabla 7-5 Resultados de la verificación de la versión de Web Server

Versión de Java ES	Número de versión de Web Server
Versión 2	6.1SP2
Versión 3	6.1SP4
Versión 4	6.1SP5
Componente de producto de la	7.0

Actualización de las dependencias de Web Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y un entorno informático) a Java ES Versión 5. Sin embargo, todos los componentes compartidos necesarios para Web Server (consulte la [Tabla 1-7 en la página 49](#)) se actualizan automáticamente mediante el programa de instalación de Java ES al realizar una actualización de Web Server a la Versión 5.

Copia de seguridad de los datos de Web Server

La actualización de Web Server de la Versión 4 a la Versión 5 no modifica los datos de configuración existentes, sino que permanecen intactos, por lo que no es necesario que realice una copia de seguridad de los datos actuales.

Obtenga las contraseñas y la información de configuración necesarias

Deberá iniciar una sesión como superusuario para realizar la actualización; además, la cuenta de usuario que realizará la migración debe tener permiso para acceder a los directorios de instalación existentes de Web Server.

Actualización de la Versión 4 de Web Server

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Web Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de Web Server a Java ES Versión 5, debe tener en cuenta las siguientes consideraciones:

- **Configurar ahora o Configurar más tarde.** Al realizar una actualización, debe especificar si desea instalar la versión de Web Server con la opción Configurar ahora o Configurar más tarde:
 - Si se utiliza la opción Configurar ahora, el programa de instalación configurará un servidor de administración o un nodo de administración, según se especifique, y creará también una configuración predeterminada y la instancia de Web Server correspondiente. Este enfoque resulta útil al realizar la instalación en un único equipo, aunque es posible que el nombre de configuración predeterminado afecte a la migración de las configuraciones de instancias existentes durante la actualización.
 - Si se utiliza la opción Configurar más tarde, el programa de instalación no realizará ninguna tarea de configuración: deberá ejecutar manualmente una secuencia de comandos `configureServer` después de proporcionar los valores de propiedades en un archivo de entrada. Este enfoque resulta útil si desea automatizar la instalación en varios equipos mediante secuencias

de comandos que realizan instalaciones silenciosas. Además, asumirá el control total de los nombres de configuración, por lo que se pueden evitar conflictos con la migración de las configuraciones de instancias existentes durante la actualización.

- **Migración de la configuración predeterminada de instancias de la Versión 4**
Al realizar una actualización, se migran los datos de configuración de cada instancia de la Versión 4 de Web Server a un almacén de configuración central que mantiene el servidor de administración de Web Server. Para realizar esta migración, se utiliza el comando `wadm migrate-server` o la consola de administración de la Versión 5.

Si la instancia que se va a migrar es la instancia predeterminada de la Versión 4 de Web Server (6.x), presentará el mismo nombre (*hostName.domainName*) que la configuración predeterminada de la Versión 5 de Web Server (7.0), que se crea automáticamente con la opción Configurar ahora.

Existen tres enfoques que describen cómo realizar la migración de la configuración de instancias predeterminada de la Versión 4 a la Versión 5; cada uno de ellos da como resultado un nombre de configuración diferente.

El enfoque que seleccione puede afectar a la actualización posterior de las aplicaciones web implementadas. Por ejemplo, para realizar la actualización de los componentes implementados de Java ES (como, por ejemplo, Access Manager y Portal Server) y los componentes Sun Java Communications Suite (como, por ejemplo, Communications Express, Instant Messaging y Delegated Administrator), es necesario que la persona que realice estas actualizaciones conozca el nombre de la configuración de la Versión 5 a la que se haya migrado la configuración de instancias de la Versión 4.

A continuación, se muestran estos tres enfoques:

- Especifique un *nuevo* nombre de configuración distinto del predeterminado, como, por ejemplo, "JavaESapps". A continuación, el comando `migrate-server` creará una nueva configuración con el nombre JavaESapps.

Posteriormente, las aplicaciones web actualizadas deberán implementarse de nuevo en la configuración JavaESapps.

- No especifique un nuevo nombre de configuración, aunque debe eliminar la nueva instancia y configuración predeterminadas de la Versión 5 (*hostName.domainName*) antes de ejecutar el comando `migrate-server`. El comando `migrate-server` creará, a continuación, una nueva configuración con el nombre predeterminado (*hostName.domainName*). La secuencia será la siguiente (consulte `wadm help` para obtener información):

```
wadm delete-instance
wadm delete-config
wadm migrate-server
wadm create-instance
```

Posteriormente, las aplicaciones web actualizadas deberán implementarse de nuevo en la configuración *hostName.domainName* , que es igual al nombre de la instancia predeterminada de la Versión 4.

- No especifique un nombre de configuración nuevo ni elimine la nueva configuración predeterminada de la Versión 5. El comando `migrate-server` creará, a continuación, una nueva configuración con el siguiente nombre: *hostName.domainName-1*.

Posteriormente, las aplicaciones web actualizadas deberán implementarse de nuevo en la configuración *hostName.domainName-1* .

El enfoque que elija para migrar las configuraciones de instancias de la Versión 4 debe comunicarse a la persona que realice la actualización posterior de una aplicación web implementada.

- **Migración de los datos de configuración.** Al migrar las configuraciones de instancias de la Versión 4, se migra automáticamente la siguiente información:
 - Toda la información de configuración del directorio de instancias de la Versión 4 de Web Server: *WebServer6-base/https-instanceName/config*. Se incluye la información de configuración de todas las aplicaciones web implementadas en la instancia de la Versión 4 (por ejemplo, los componentes de Java ES como Access Manager y Portal Server).
 - La información de acl de *WebServer6-base/httpacl*
 - La información de auth-db de *WebServer6-base/userdb*
 - La información del programador de actividades de *WebServer6-base/httpacl*
 - La información de certificados de *WebServer6-base/alias*
 - La información de las recopilaciones de búsquedas y los archivos de índices, tal y como se especificó al realizar la migración.

La migración automática *no* incluye los siguientes datos:

- El contenido de docroot. En su lugar, la nueva configuración señalará al antiguo docroot y se registrará un mensaje en el registro de migración.
- Los datos de Webdav. Se migrará la información de recopilación de Webdav.

- No se migrarán los complementos NSAPI de terceros. En su lugar, señalarán al archivo de la Versión 4 y se registrará un mensaje en el registro de migración.
- Los archivos de registro.
- Los cambios en el docroot de la recopilación de búsqueda.
- Las secuencias de comandos de línea de comandos (startsvr, startsvr.bat, stopsvr, stopsvr.bat, restart, reconfig y reconfig.bat).

Para obtener información acerca de la migración de los datos, consulte *Web Server 7.0 Installation and Migration Guide*, <http://docs.sun.com/doc/819-2625>.

- **Creación de las instancias de la Versión 5 de Web Server.** Una vez realizada la migración, debe crear de forma explícita una instancia de la Versión 5 de Web Server que se corresponda con la instancia migrada de la Versión 4. Esta operación no se realiza automáticamente.

Procedimiento de actualización

El procedimiento descrito a continuación hace referencia a todas las instancias de Web Server que se corresponden con la misma imagen de Web Server instalada en el equipo en el que se va a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Detenga todas las instancias de Web Server y del servidor de administración que se estén ejecutando.

WebServer6-base/https-instanceName/stop

WebServer6-base/https-admserv/stop

3. Realice una nueva instalación de la Versión 5 de Web Server.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b. Seleccione Web Server en la página de selección de componentes.
- c. Especifique una ruta de instalación distinta de la ruta de la Versión 4 de Web Server.
- d. Seleccione Configurar ahora o Configurar más tarde.
 - Si selecciona Configurar ahora, vaya al [Paso e](#).
 - Si selecciona Configurar más tarde, vaya al [Paso f](#).
- e. Si decide utilizar la opción Configurar ahora, el programa de instalación de Java ES ofrecerá dos opciones:
 - Configurar la instancia de administración como servidor de administración
Utilice esta opción en el equipo que alojará el servidor de administración necesario para realizar la migración de las instancias de la Versión 4 a la Versión 5, entre otras tareas administrativas.
 - Configurar la instancia de administración como nodo de administración
Utilice esta opción en un equipo que vaya a alojar una instancia de Web Server remota en relación con el servidor de administración. La instancia de administración se configura como un agente del nodo que interactúa con el servidor de administración.
- i. Especifique los valores de configuración solicitados.

Se le pedirá que especifique el nombre de host y el puerto HTTP, así como el nombre de usuario y la contraseña de administración.
- ii. Confirme las opciones de instalación seleccionadas.

Se instalarán los paquetes de Web Server y se mostrará un resumen de la instalación.

El programa de instalación de Java ES creará una configuración predeterminada con el nombre *hostName.domainName* y la instancia de Web Server correspondiente.

- III. Salga del programa de instalación de Java ES y vaya al [Paso 4 en la página 155](#).
- f. Si decide utilizar la opción Configurar más tarde, el programa de instalación de Java ES creará una secuencia de comandos `configureServer` que se debe ejecutar en el [Paso IV en la página 155](#).

- I. Confirme las opciones de instalación seleccionadas.

Se instalarán los paquetes de Web Server y se mostrará un resumen de la instalación.

- II. Salga del programa de instalación de Java ES.

- III. Establezca los valores del archivo `WebServer7-base/setup/WSInstall.properties`.

Proporcione los valores para todas las propiedades necesarias (no opcionales) de la siguiente tabla.

Tabla 7-6 Valores de `WSInstall.properties`

Propiedad	Descripción
<code>WS_DOCROOT</code>	(Opcional) Ubicación de los documentos que pueden alojar los archivos de contenido web.
<code>WS_SERVER_NAME</code>	Nombre de host que puede utilizarse para atender las solicitudes HTTP.
<code>WS_SERVER_USER</code>	Id. de usuario en tiempo de ejecución de Unix. Entre los valores válidos, se incluyen <code>root</code> , cualquier usuario válido de UNIX y <code>webservd</code> (valor predeterminado).
<code>WS_HTTP_PORT</code>	Puerto de la instancia que puede utilizarse para recibir las solicitudes HTTP.
<code>WS_ADMIN_SSL_PORT</code>	Puerto SSL de administración.
<code>WS_ADMIN_HOST</code>	Nombre del host de administración para las tareas del servidor de administración.

Tabla 7-6 Valores de WSInstall.properties *(continúa)*

Propiedad	Descripción
WS_CONFIG_NAME	Nombre de configuración para este host. Este valor puede ser igual al que se especificó en WS_SERVER_NAME
WS_ADMIN_SERVER_USER	Usuario en tiempo de ejecución de UNIX del servidor de administración. Valores válidos: "root" o el mismo usuario que WS_SERVER_USER.
WS_ADMIN_LOGIN_USER	Nombre de usuario de inicio de sesión del servidor de administración.
WS_ADMIN_LOGIN_PASSWORD	Contraseña de inicio de sesión del servidor de administración.
WS_ADMIN_HTTP_PORT	(Opcional) Puerto de administración que no sea SSL. Valor predeterminado: 8800
WS_START_ON_BOOT	(Opcional) Función de inicio durante el arranque (true/false) Si se especifica True (verdadero), la instancia del servidor y su servidor de administración se iniciarán automáticamente después de rearrancar el sistema. Valor predeterminado: falso
WS_64BIT_INSTALL	(Opcional) Modo de tiempo de ejecución del servidor (true/false) Si se especifica True (verdadero), se configurará el servidor en el modo de 64 bits. (Sólo para Solaris). Si se especifica False (falso), se configurará el servidor en el modo de 32 bits. (Sólo para Solaris) Valor predeterminado: falso
WS_ADMIN_IS_SERVER_MODE	(Opcional) Modo de configuración de la administración. (true/false). Si se especifica True (verdadero), se configurará el servidor en el modo de servidor de administración. Si se especifica False (falso), se configurará el servidor en el modo de agente de administración. Valor predeterminado: true (verdadero)
WS_REGISTER_ADMIN_AGENT	(Opcional) Registro del agente remoto. (true/false). Sólo es necesario si WS_ADMIN_IS_SERVER_MODE se ha establecido en "false" (falso). Si se especifica True (verdadero), deberá proporcionar el host del servidor de administración remoto para el registro. Valor predeterminado: true (verdadero)

Tabla 7-6 Valores de `WSInstall.properties` (continúa)

Propiedad	Descripción
<code>WS_AGENT_SSL_PORT</code>	(Opcional) Puerto SSL del agente de administración. Sólo es necesario si <code>WS_ADMIN_IS_SERVER_MODE</code> se ha establecido en <code>false</code> (falso).
<code>WS_AGENT_HOST=</code>	(Opcional) Nombre de host del agente de administración. Sólo es necesario si <code>WS_ADMIN_IS_SERVER_MODE</code> se ha establecido en <code>false</code> (falso).

IV. Ejecute la secuencia de comandos `configureServer`.

```
WebServer7-base/setup/configureServer
-inputfile WebServer7-base/setup/WSInstall.properties
-logfile WebServer7-base/setup/WSInstall.log
-verbose
```

La secuencia de comandos `configureServer` creará una configuración predeterminada con el nombre `hostName.domainName` y la instancia de Web Server correspondiente.

4. Inicie el servicio del servidor de administración de Web Server.

```
WebServer7Config-base/admin-server/bin/startserv
```

5. Migre las configuraciones de instancias de la Versión 4 de Web Server a las configuraciones de la Versión 5.

Puede utilizar la línea de comandos (`wadm`) o las herramientas de administración de la interfaz gráfica de usuario (inicie una sesión en la GUI del servidor de administración de Web Server). Los pasos siguientes se basan en la interfaz de línea de comandos `wadm`.

Por ejemplo, para migrar una instancia con el nombre `myinstance` a una nueva configuración:

```
WebServer7-base/bin/wadm migrate-server --user=admin
--host=localhost --server-root=/opt/SUNWwbsvr
--instance=https-myinstance --config=newconfigname
```

La sintaxis completa del comando es la siguiente:

```
WebServer7-base/bin/wadm migrate-server

--user=admin-user [--password-file=admin-pswd-file] [--host=admin-host]
[--echo] [--rcfile=rcfile] [--no-prompt] [--verbose]

[--search-collection-copy-path=searchCollectionPath]
[--log-dir=directory] --serverroot=path
([--all] | [--instance=https-instanceName] [--config=newconfigName])
```

En el ejemplo anterior, el primer conjunto de opciones de comandos es común a todos los comandos de wadm y se describe, a continuación, en la [Tabla 7-7](#). El segundo conjunto de opciones de comandos es específico del comando "migrate-server" y se describe en la [Tabla 7-8](#).

Si llama a wadm con sólo el primer conjunto de opciones de comandos, accederá al shell de comandos de wadm. Para llamar a los comandos de este shell, no es necesario que especifique de nuevo las opciones comunes.

Si llama a los comandos de wadm completos desde fuera del shell, deberá especificar, como mínimo, las opciones --user y --host. (Si omite la opción --password-file, se le solicitará que introduzca una contraseña; si omite el resto de opciones, se supondrá que se debe utilizar el valor predeterminado.) No obstante, no se han incluido las opciones --user y --host para los comandos que ilustran los procedimientos de este capítulo para simplificar la explicación del proceso.

wadm utiliza de forma predeterminada el protocolo SSL en el puerto 8989.

Para obtener información completa sobre los comandos y las opciones de wadm, consulte *Web Server 7.0 CLI Reference Manual*, <http://docs.sun.com/doc/819-3283>.

Tabla 7-7 Opciones de comandos comunes de wadm

Opción	Descripción
user	Id. de usuario administrativo de Web Server autorizado.
password-file	El archivo que contiene las contraseñas para la autenticación del usuario administrativo en el servidor de administración. El archivo de contraseñas contiene una línea WADM_PASSWORD=password. Si no se especifica esta opción en el comando, se le solicitará que introduzca la contraseña.
host.	Nombre del equipo en el que se está ejecutando el servidor de administración. Valor predeterminado: localhost.

Tabla 7-7 Opciones de comandos comunes de wadm *(continúa)*

Opción	Descripción
echo	Si se establece esta opción en true (verdadero), se repetirá la línea de comandos en la salida estándar antes de ejecutar el comando. Valor predeterminado: falso
interactive	Si esta opción se establece en true (verdadero), se le solicitará que introduzca las opciones de contraseña necesarias. Valor predeterminado: true (verdadero).
rcfile	Archivo de inicio que se utilizará para la carga durante el inicio de wadm. Valor predeterminado: ~/.wadmrc.
no-prompt	Si esta opción se establece en true (verdadero), el comando no le pedirá nunca ninguna entrada de usuario bajo ninguna circunstancia. Por ejemplo, el comando simplemente mostrará un error si, al llamarlo, faltan parámetros, en lugar de solicitar y esperar la entrada de usuario. Es posible que desee establecer esta opción en true (verdadero) al utilizar los comandos de wadm con una secuencia de comandos de shell, ya que el comando devuelve siempre la entrada de usuario en lugar de esperar su recepción. Valor predeterminado: false (falso).
verbose	Si se establece en true (verdadero), aparece una lista detallada. Valor predeterminado: false (falso).

Tabla 7-8 Opciones y operandos del comando `wadm migrate-server`

Opción/operando	Descripción
search-collection-copy-path	Especifica la ruta en la que se copiarán los archivos de índices de las recopilaciones de búsqueda al migrar estas recopilaciones. Pueden producirse los siguientes escenarios de migración: Si la ruta de la recopilación de búsqueda de Web Server 6.x se encuentra fuera de la instancia de Web Server 6.x, la ruta de la recopilación de búsqueda migrada señalará a la ruta de la recopilación de búsqueda de Web Server 6.x y se omitirá esta opción. Si la ruta de la recopilación de búsqueda de Web Server 6.x se encuentra en la instancia de Web Server 6.x, se especificará una ruta válida para esta opción y los archivos de índices de la recopilación de búsqueda se copiarán en el siguiente directorio: <i>searchCollectionPath/configName/virtualServerName/collectionName</i>. Si la ruta especificada no es válida, se registrará un mensaje de error. Si la ruta de la recopilación de búsqueda de Web Server 6.x se encuentra en la instancia de Web Server 6.x, pero no se ha especificado ninguna ruta para esta opción, los archivos de índices de la recopilación de búsqueda no se copiarán. Se escribirá un mensaje en el registro de migración solicitando al usuario que copie manualmente los archivos de índices de la recopilación de búsqueda mediante el comando <code>wadm add-documents</code>. En ese caso, la ruta de la recopilación de búsqueda migrada será la siguiente: <i>WebServer7Config-base/https-configName/config/collections/virtualServerName/collectionName</i>.
log-dir	La ubicación del registro de migración. Valor predeterminado: <i>WebServer7Config-base/admin-serv/logs</i>
serverroot	La ubicación (directorio) de instalación en la que se ha instalado la versión Web Server 6.x: la misma que <i>WebServer6-base</i>.
all	Si se establece en <code>true</code> (verdadero), todas las configuraciones de instancias de Web Server 6.x se migrarán a las configuraciones de Web Server 7.0 con los mismos nombres que las instancias. Si ya existe una configuración con ese nombre, <i>instanceName-1</i> se utilizará como nombre de configuración. Valor predeterminado: <code>false</code> (falso).
instance	Si deben migrarse individualmente las configuraciones de instancias (el valor de <code>"all"</code>=<code>false</code>), se trata del nombre de la configuración de instancias de Web Server 6.x que se va a migrar (con el formato:<i>https-instanceName</i>). El nombre de instancia predeterminado de Web Server 6.x es <i>hostName.domainName</i>.

Tabla 7-8 Opciones y operandos del comando `wadm migrate-server` (continúa)

Opción/operando	Descripción
config	El nombre de la configuración a la que se va a migrar la configuración de instancias de Web Server 6.x especificada. Se utiliza de forma predetermina el nombre de la instancia (<i>instanceName</i>) de la configuración de instancias de Web Server 6.x. Sin embargo, si ya existe una configuración con ese nombre, el comando anexará un entero al nombre. Es posible que se produzca este escenario si va a migrar la configuración de instancias predeterminada de Web Server 6.x.

Al utilizar el comando `migrate-server`, tenga en cuenta las siguientes consideraciones:

- Si desea migrar varias configuraciones de instancias de la Versión 4, puede ejecutar el comando `migrate-server` varias veces con diferentes valores para `--instance` y los argumentos de `--config` correspondientes o utilizar la opción `--all` para migrarlas todas de forma simultánea.
- Para cada llamada al comando "migrate-server", se creará, durante la migración, un archivo de registro con el siguiente nombre en el directorio especificado por la opción `--log-dir` (o en el directorio predeterminado `WebServer7Config-base/admin-server/logs`):

`MIGRATION_aaaaammdhlhmmss.log`

Si selecciona la opción `--all`, el archivo de registro almacenará la información de configuración de todas las instancias migradas.
- Para todos los datos que no se migren con el comando `migrate-server` (consulte [“Consideraciones sobre la actualización” en la página 148](#)), deberá realizar la migración manualmente (consulte [“Tareas posteriores a la actualización” en la página 163](#)).

6. Cree las instancias de la Versión 5 de Web Server.

Debe crear una nueva instancia de la Versión 5 para cada configuración de instancias de la Versión 4 que se haya migrado en el [Paso 5](#). (Si se ha realizado una migración a la configuración predeterminada, ya existirá la instancia predeterminada correspondiente, por lo que puede saltar al [Paso c.](#))

- a.** Antes de crear una nueva instancia, verifique el registro de migración y solucione todos los problemas que haya en la configuración migrada.

- b. Ejecute el comando create-instance.

```
WebServer7-base/bin/wadm create-instance  
--config=configName nodehost1 [nodehost2 ...nodehostN]
```

Las opciones de comandos comunes se describen en la [Tabla 7-7 en la página 156](#). Las opciones específicas del comando create-instance se describen en la siguiente tabla.

Tabla 7-9 Opciones y operandos del comando `wadm create-instance`

Opción/operando	Descripción
<code>o</code>	
<code>config</code>	El nombre de la configuración de la Versión 5 a la que debería señalar la instancia.
<code>nodehost</code>	Nombre del equipo en el que se va a crear la instancia. Puede especificar varios equipos en una lista separada por espacios con el formato <i>hostName.domainName</i> , creando de esta forma varias instancias idénticas.

El comando `create-instance` crea un directorio de instancias en *WebServer7Config-base/https-configName* en los nodos especificados e implementa la configuración en los directorios de instancias correspondientes.

- c. Si la instancia de destino ya existe como instancia predeterminada, sólo tiene que implementar la configuración correspondiente, sin necesidad de crear, en primer lugar, la instancia:

```
WebServer7-base/bin/wadm deploy-config
[--force] [--restart] [--no-reconfig]
configName
```

Las opciones de comandos comunes se describen en la [Tabla 7-7 en la página 156](#). Las opciones específicas del comando `deploy-config` se describen en la siguiente tabla.

Tabla 7-10 Opciones y operandos del comando `wadm deploy-cofig`

Opción/operando	Descripción
<code>force</code>	Si se establece en <code>true</code> (verdadero), se sobrescribe de forma forzosa la configuración que se ha modificado manualmente desde la anterior implementación de la configuración. Valor predeterminado: <code>false</code>
<code>restart</code>	Si se establece en <code>true</code> (verdadero), las instancias que se están ejecutando se reiniciarán para obtener los valores de la configuración implementada. Valor predeterminado: <code>false</code>
<code>no-reconfig</code>	Si se establece en <code>true</code> (verdadero), las instancias que se están ejecutando no obtendrán los valores de la configuración implementada hasta que se reinicie la instancia. Valor predeterminado: <code>false</code>

Tabla 7-10 Opciones y operandos del comando `wadm deploy-cofig`

Opción/operando	Descripción
<code>configName</code>	El nombre de la configuración de la Versión 5 que se va a implementar en una instancia de Web Server cuyo nombre se corresponde con el nombre de configuración.

7. Inicie todas las instancias de la Versión 5.

`WebServer7Config-base/https-configName/bin/startserv`

La secuencia de comandos `startserv` se crea durante la creación de la instancia. Si la instancia se inicia sin ningún problema, aparecerá un mensaje en el que se indica “successful server startup” (el servidor se ha iniciado satisfactoriamente). Se mostrará la URL predeterminada de la instancia.

Verificación de la actualización

Puede verificar la actualización de Web Server a la Versión 5 mediante los siguientes pasos:

1. Compruebe si hay mensajes de `ERROR` en el archivo de registro de migración que se acaba de crear.

Si es necesario, realice los cambios manuales pertinentes (consulte “[Tareas posteriores a la actualización](#)” en la página 163).

2. Verifique las instancias de la Versión 5 de Web Server.

Desde un navegador web, acceda a la siguiente URL y asegúrese de que se muestre la página de bienvenida:

`http://hostName.domainName:port`

donde el nombre de host completo y el puerto se corresponden con cada instancia. También puede cortar la siguiente URL y pegarla en el navegador:

`WebServer7Config-base/https-configName/bin/startserv`

3. Ejecute la instancia de Web Server con la opción `-version`:

`WebServer7Config-base/https-configName/bin/startserv -version`

Consulte la [Tabla 7-5 en la página 147](#) para obtener los valores de salida de la versión.

Tareas posteriores a la actualización

La principal tarea posterior a la actualización consiste en realizar la migración manual de determinados datos de la Versión 4, si es necesario. Normalmente son datos asociados a uno o varios servidores virtuales que se han configurado para la Versión 4 y se han especificado en el archivo de configuración `server.xml`.

Tenga en cuenta los procedimientos posteriores a la actualización necesarios para abordar las siguientes situaciones:

- [Migración del contenido de docroot de Web Server 6.1](#)
- [Migración de la información de recopilación de webdav](#)
- [Migración de los archivos de registro](#)
- [Migración de los complementos NSAPI de terceros](#)
- [Cambio de la raíz de documentos de las recopilaciones de búsqueda](#)
- [Personalización de las secuencias de comandos de línea de comandos](#)

Migración del contenido de docroot de Web Server 6.1

1. Copie el contenido de docroot de Web Server 6.1 en la ubicación que desee.
2. Actualice la nueva ruta de la raíz de documentos utilizando el siguiente comando:

```
WebServer7-base/bin/wadm set-virtual-server-prop
--config=configName --vs=virtualServerName
document-root=nueva ruta de docroot
```

Las opciones de comandos comunes se describen en la [Tabla 7-7 en la página 156](#). Las opciones específicas del comando `set-virtual-server-prop` se describen en la siguiente tabla.

Tabla 7-11 Opciones y operandos del comando `wadm set-virtual-server-prop`

Opción/operando	Descripción
config	El nombre de la configuración de la Versión 5 para la que se va a establecer la nueva ruta de la raíz de documentos.
vs	El nombre del servidor virtual correspondiente a la raíz de documentos migrada.
document-root	La ruta al nuevo directorio raíz de documentos.

3. Vuelva a implementar la configuración en las instancias de Web Server pertinentes.

```
WebServer7-base/bin/wadm deploy-config  
[--force] [--restart] [--no-reconfig]  
configName
```

Las opciones de comandos se describen en la [Tabla 7-10 en la página 161](#).

Migración de la información de recopilación de webdav

No es necesario realizar ninguna migración manual adicional. Sólo se debe actualizar la ruta de docroot.

Migración de los archivos de registro

Copie estos archivos en una ubicación conocida si desea guardarlos (de lo contrario, se borrarán si elimina la instalación de la Versión 4).

Migración de los complementos NSAPI de terceros

1. Copie los archivos de biblioteca desde la ubicación de la Versión 4 al directorio `WebServer7-base/lib`.
2. Exporte los archivos de configuración `magnus.conf` y `obj.conf` a un directorio temporal.

```
WebServer7-base/bin/wadm get-config-file --config=configName  
magnus.conf > /tmp/magnus.conf
```

```
WebServer7-base/bin/wadm get-config-file --config=configName  
obj.conf > /tmp/obj.conf
```

Las opciones de comandos comunes se describen en la [Tabla 7-7 en la página 156](#).

3. Modifique los archivos `magnus.conf` y `obj.conf`, como se especifica en la documentación de los complementos NSAPI de terceros.
4. Importe los archivos de configuración `magnus.conf` y `obj.conf` desde el directorio temporal.

```
WebServer7-base/bin/wadm set-config-file --config=configName  
--upload-file=/tmp/magnus.conf magnus.conf
```

```
WebServer7-base/bin/wadm set-config-file --config=configName  
--upload-file=/tmp/obj.conf obj.conf
```

Las opciones de comandos comunes se describen en la [Tabla 7-7 en la página 156](#).

5. Vuelva a implementar la configuración modificada en las instancias de Web Server pertinentes.

```
WebServer7-base/bin/wadm deploy-config
[--force] [--restart] [--no-reconfig]
configName
```

Las opciones de comandos se describen en la [Tabla 7-10 en la página 161](#).

Cambio de la raíz de documentos de las recopilaciones de búsqueda

El comando "migrate-server" incluye una opción para migrar la información de las recopilaciones de búsqueda. Sin embargo, es posible que desee cambiar la raíz de documentos de las recopilaciones de búsqueda, como se indica a continuación:

1. Si la raíz de documentos de la recopilación de búsqueda es diferente de la utilizada para la Versión 4, utilice el siguiente comando para establecer la raíz de documentos para la recopilación de búsqueda:

```
WebServer7-base/bin/wadm set-search-collection-prop
--config=configName --vs=virtualServerName
--collection-name=searchCollectionName document-root=nueva ruta de docroot
para la recopilación de búsqueda
```

Las opciones de comandos comunes se describen en la [Tabla 7-7 en la página 156](#). Las opciones específicas del comando set-search-collection-prop se describen en la siguiente tabla.

Tabla 7-12 Opciones y operandos del comando wadm set-search-collection-prop

Opción/operando	Descripción
config	El nombre de la configuración de la Versión 5 para la que se va a establecer la nueva ruta de la raíz de documentos de la recopilación de búsqueda.
vs	El nombre del servidor virtual correspondiente a la recopilación de búsqueda.
collection-name	El nombre de la recopilación de búsqueda para la que se va a establecer la nueva ruta de la raíz de documentos.
document-root	La ruta al nuevo directorio raíz de documentos para la recopilación de búsqueda.

2. Vuela a implementar la configuración en las instancias de Web Server pertinentes.

```
WebServer7-base/bin/wadm deploy-config
[--force] [--restart] [--no-reconfig]
configName
```

Las opciones de comandos se describen en la [Tabla 7-10 en la página 161](#).

Personalización de las secuencias de comandos de línea de comandos

Si se han personalizado las secuencias de comandos como, por ejemplo, `startsvr`, `startsvr.bat`, `stopsvr`, `stopsvr.bat`, `restart`, `reconfig` y `reconfig.bat` deberá realizar las mismas personalizaciones en las secuencias de comandos predeterminadas de la versión, que se encuentran en el siguiente directorio:
`WebServer7-base/bin`.

Anulación de la actualización

La nueva instalación de la Versión 5 y la posterior migración de las configuraciones de instancias de Web Server dejan intacta la Versión 4 de Web Server. Por lo tanto, para anular la Versión 5 de Web Server, sólo es necesario realizar los siguientes pasos para restablecer la Versión 4.

1. Inicie sesión como root o conviértase en superusuario.

```
su -
```

2. Detenga, una a una, todas las instancias de Web Server que se estén ejecutando.

```
WebServer7Config-base/https-configName/bin/stopserv
```

Si el servidor se ha detenido correctamente, aparecerá el mensaje “server has been shutdown” (se ha cerrado el servidor).

3. Elimine la instalación de la Versión 5 de Web Server.

Debe eliminar todas las instancias y las configuraciones migradas de la Versión 5:

- a. Elimine todas las instancias de la Versión 5.

```
WebServer7-base/bin/wadm delete-instance --user ...
--config=configName hostName.domainName
```

- b. Elimine todas las configuraciones de la Versión 5.

```
WebServer7-base/bin/wadm delete-config --user ... configName
```

4. Reinicie las instancias de Web Server que se habían detenido al actualizar Web Server, como se describe en [“Procedimiento de actualización” en la página 151](#).

Actualización de Web Server desde Java ES Versión 3

El procedimiento de actualización del componente Web Server de Java ES 2005Q1 (Versión 3) a la Versión 5 es igual al procedimiento de actualización de la Versión 4 de Web Server a la Versión 5.

Para actualizar Web Server de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en “[Actualización de Web Server desde Java ES Versión 4](#)” en la [página 146](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Actualización de Web Server desde Java ES Versión 2

El procedimiento de actualización del componente Web Server de Java ES 2004Q2 (Versión 2) a la Versión 5 es igual al procedimiento de actualización de la Versión 4 de Web Server a la Versión 5.

Para actualizar Web Server de la Versión 2 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Web Server desde Java ES Versión 4”](#) en la [página 146](#) y sustituya la referencia a la Versión 4 por la Versión 2.

Java DB

En este capítulo, se describe cómo actualizar Java DB a Java ES 5 (Versión 5): Java DB 10.1.3.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de las actualizaciones de Java DB” en la página 172
- “Actualización de Java DB desde Java ES Versión 4” en la página 174

NOTA

Las ubicaciones de los archivos de este capítulo se especifican en relación con la ruta de directorio a la que se denomina *JavaDB-base*. Esta ruta fue establecida por el programa de instalación de Java ES cuando se instaló Java DB.

Los valores predeterminados de esta ruta de directorio se muestran en la siguiente tabla.

Tabla 8-1 Java DB Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>JavaDB-base</i>	/opt/SUNWjavadb	/opt/sun/javadb

Visión general de las actualizaciones de Java DB

En esta sección se describen los siguientes aspectos generales de Java DB que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Java ES Versión 5](#)
- [Guía de actualización deJava ES Versión 5](#)
- [Datos de Java DB](#)
- [Estrategia de actualización para Java DB](#)

Acerca de Java ES Versión 5

Java DB de Java ES Versión 5 es la primera versión disponible de un componente de producto de Java ES; Java DB estuvo al principio disponible como un componente compartido de DerbyDatabase, incluido en Java ES Versión 4.

La Versión 5 de Java DB representa una versión inferior con respecto a la Versión 4. Incluye algunas funciones mejoradas, interfaces actualizadas y soluciones de errores exclusivas.

Guía de actualización deJava ES Versión 5

La [Tabla 8-2](#) muestra las rutas de actualización compatibles de Java DB para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 8-2 Rutas de actualización a Java ES 5 (Versión 5): Java DB 10.1.3

Versión de Java ES	Versión de Java DB		
	Java DB Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Derby Database 10.0.2	Actualización directa: Sustituya la Versión 4 con una nueva instalación. Los datos persistentes no se ven afectados.	Ninguna

Datos de Java DB

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Java DB.

Tabla 8-3 Uso de datos de Java DB

Tipo de datos	Ubicación	Uso
Datos de configuración	La configuración de la instancia es específica de la aplicación, no se almacena en <i>JavaDB-base</i> y no se ve afectada por la actualización.	Configuración de la instancia de Java DB
Datos persistentes	Los directorios de las bases de datos y sus contenidos son específicos de la aplicación y no se almacenan en <i>JavaDB-base</i> .	Bases de datos y certificados de usuario

Estrategia de actualización para Java DB

La estrategia utilizada para la actualización de Java DB depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Java DB presentando una serie de problemas que pueden influir en el plan de actualización de Java DB.

Problemas de compatibilidad

La Versión 5 de Java DB es compatible con la Versión 4.

Dependencias

Java DB sólo tiene una dependencia con respecto al componente compartido J2SE (consulte la [Tabla 1-7 en la página 49](#)).

Actualización de Java DB desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Java DB desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Java DB](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Java DB de la Versión 4 a la Versión 5 de Java ES, hay que tener en cuenta los siguientes aspectos del proceso de actualización:

- **Enfoque general de actualización.** La actualización se consigue llevando a cabo una nueva instalación de la Versión 5 que sustituya a la Versión 4 de Java DB. Los datos y la configuración de la Versión 4 permanecen intactos.
- **Dependencias de actualización.** Java DB tiene una dependencia fuerte de actualización con el componente compartido J2SE (consulte la [Tabla 1-7 en la página 49](#)); dicho componente se actualiza automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando se realiza una actualización de Java DB.
- **Compatibilidad con versiones anteriores.** La Versión 5 de Java DB es totalmente compatible con la Versión 4.
- **Anulación de la actualización.** No se puede deshacer la actualización a la Versión 5, pero puede restablecer una copia de seguridad de la instalación de la Versión 4.
- **Problemas de plataforma.** El enfoque general de actualización de Java DB es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de Java DB

En esta sección se describe cómo realizar una actualización de Java DB de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. En esta sección, se describen los siguientes temas:

- Tareas previas a la actualización
- Actualización de la Versión 4 de Java DB
- Verificación de la actualización
- Tareas posteriores a la actualización
- Anulación de la actualización

Tareas previas a la actualización

Antes de actualizar el software de Java DB, debe realizar las tareas descritas a continuación:

- Verifique la información sobre la versión actual
- Actualización de las dependencias de Java DB
- Copia de seguridad de los datos de Java DB
- Obtenga las contraseñas y la información de configuración necesarias

Verifique la información sobre la versión actual

Para verificar la versión actual de Java DB, utilice el siguiente comando:

```
java -cp JavaDB-base/lib/derby.jar org.apache.derby.tools.sysinfo
```

En la siguiente tabla se muestra la información sobre la versión (para el archivo derby.jar):

Tabla 8-4 Resultados de la verificación de la versión de Java DB

Versión de Java ES	Número de versión de Java DB
Versión 4	10.0.2.1
Componente de producto de la	10.1.3.1

Actualización de las dependencias de Java DB

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que necesita Java DB cuando se realiza la actualización a la Versión 5 de Java DB.

Copia de seguridad de los datos de Java DB

Al actualizar Java DB de la Versión 4 a la Versión 5, no se modifican los datos de configuración ni los datos persistentes, por lo que no es necesario que realice una copia de seguridad de los datos actuales. Sin embargo, tendrá que hacer una copia de seguridad de toda la instalación de Java DB y de los datos para garantizar la seguridad.

Obtenga las contraseñas y la información de configuración necesarias

No se necesita ninguna contraseña ni información de configuración para actualizar Java DB.

Actualización de la Versión 4 de Java DB

En esta sección se describe el procedimiento de actualización en las plataformas Solaris y Linux.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia a todas las instancias de Java DB que residen localmente en el equipo en el que vaya a realizarse la actualización.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Detenga la Versión 4 de Java DB.

Si está ejecutando un servidor de red, utilice el siguiente comando:

```
java -cp JavaDB-base/lib/derby.jar:JavaDB-base/lib/derbynet.jar  
org.apache.derby.drda.NetworkServerControl shutdown
```

En caso contrario, simplemente cierre todas las aplicaciones utilizando Java DB.

3. Realice una nueva instalación de la Versión 5 de Java DB.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES en el equipo que aloje la Versión 4 de Java DB.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b. Seleccione Java DB en la página de selección de componentes.
Se sobrescribirá la instalación anterior.
- c. Seleccione la opción Configurar más tarde.
No se admite Configurar ahora.
- d. Si fuera necesario, seleccione la opción para instalar paquetes traducidos.
- e. Una vez completada la instalación, salga del programa de instalación de Java ES.

4. Inicie la Versión 5 de Java DB.

Si está ejecutando un servidor de red, utilice el siguiente comando:

```
java -jar <JavaDB-base>/lib/derbynet.jar start
```

En caso contrario, simplemente inicie cualquier aplicación utilizando Java DB en modo incorporado.

Verificación de la actualización

Para comprobar que la actualización de Java DB se ha realizado correctamente, utilice los siguientes comandos:

```
java -cp JavaDB-base/lib/derby.jar org.apache.derby.tools.sysinfo
```

Consulte la [Tabla 8-4 en la página 175](#) para obtener los valores de salida (para la versión del archivo `derby.jar`).

Tareas posteriores a la actualización

Al actualizar Java DB de la Versión 4 a la 5, se deben convertir los datos de Java DB del formato de disco 10.0 al formato 10.1. Para llevar a cabo esta conversión, conéctese a la base de datos con `upgrade=true` anexo a la URL JDBC. Por ejemplo:

```
java -cp JavaDB-base/lib/derbytools.jar:JavaDB-base/lib/derby.jar
org.apache.derby.tools.ij
```

```
ij version 10.1
```

```
ij> conectar a 'jdbc:derby://databasePath;upgrade=true';
```

```
ij> salir;
```

Anulación de la actualización

No se puede deshacer la actualización a la Versión 5. Sin embargo, se pueden restablecer los datos y una copia de seguridad de la instalación de la Versión 4.

Actualización de varias instancias

En algunas arquitecturas de implementación, Java DB se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que las instancias de Java DB se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Debe realizar la actualización de Java DB en todos los equipos tal y como se describe en [“Actualización de la Versión 4 de Java DB” en la página 174](#).

Almacén de sesión de alta disponibilidad

En este capítulo se describe cómo actualizar el Almacén de sesión de alta disponibilidad a Java ES 5 (Versión 5): Almacén de sesión de alta disponibilidad (HADB) 4.4.3.

Este capítulo proporciona una visión general de los problemas de actualización antes de abordar las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de HADB” en la página 181
- “Actualización de HADB desde Java ES Versión 4” en la página 184
- “Actualización de HADB desde Java ES Versión 3” en la página 192

NOTA

Las ubicaciones de los archivos de este capítulo se especifican en relación con la ruta de directorio a la que se denomina *HADB-base*. Debe haberse especificado, al menos, parte de esta ruta como directorio de instalación durante la instalación inicial de HADB. De lo contrario, el programa de instalación asigna un valor predeterminado.

El valor predeterminado de *HADB-base* no depende de la plataforma del sistema operativo, como se muestra en la siguiente tabla.

Tabla 9-1 HADB Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>HADB-base</i> Programa de instalación de Java ES	<i>/opt/SUNWhadb/version_number</i>	<i>/opt/SUNWhadb/version_number</i>
<i>HADB-base</i> programa de instalación independiente de Application Server 8.2 EE	<i>/opt/SUNWappserver/appserver</i> <i>/hadb/version_number</i>	<i>/opt/SUNWappserver/appserver</i> <i>/hadb/version_number</i>

Visión general de la actualización de HADB

En esta sección se describen los siguientes aspectos generales de HADB que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de HADB de Java ES Versión 5](#)
- [Guía de actualización de HADB](#)
- [Datos de HADB](#)
- [Estrategia de actualización para HADB](#)

Acerca de HADB de Java ES Versión 5

Java ES Versión 5 de las versiones de HADB presenta mejoras menores para el usuario en relación con la Versión 4 de HADB.

Guía de actualización de HADB

La [Tabla 9-2](#) muestra las rutas de actualización compatibles de HADB para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 9-2 Rutas de actualización a Java ES 5 (Versión 5): HADB 4.4.3

Versión de Java ES	HADB Versión	Enfoque general	Reconfiguración necesaria
Versión 4	HADB 4.4.2 (2005Q4)	Actualización directa: Está disponible un enfoque de actualización en línea y otro de actualización sin conexión.	Ninguna
Versión 3	HADB 4.4.1 (2005Q1)	Actualización directa: Está disponible un enfoque de actualización en línea y otro de actualización sin conexión.	Ninguna
Versión 2	HADB 4.4.0-14 (2004Q2)	Actualización no admitida.	Ninguna
Versión 1	No disponible	Sin actualización	Ninguna

Tabla 9-2 Rutas de actualización a Java ES 5 (Versión 5): HADB 4.4.3

Versión de Java ES	Versión de HADB		
	HADB Versión	Enfoque general	Reconfiguración necesaria
Versiones anteriores de Java ES	No disponible	Sin actualización	Ninguna

Datos de HADB

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de HADB.

Tabla 9-3 Uso de datos de HADB

Tipo de datos	Ubicación	Uso
Datos de aplicación dinámicos	/var/opt/SUNWhadb and /etc/opt/SUNWhadb	Información sobre el Almacén de sesión de alta disponibilidad y de configuración.

Estrategia de actualización para HADB

La estrategia utilizada para la actualización de HADB depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a HADB presentando una serie de problemas que pueden influir en el plan de actualización de HADB.

Problemas de compatibilidad

La Versión 5 de HADB es compatible con HADB incluido en Java ES Versión 4.

HADBDependencias

La Versión 5 de HADB sólo presenta relaciones de dependencia con el componente compartido J2SE: Java™ 2 Platform, Standard Edition (J2SE™) Versión 1.4 o posterior.

Actualización de HADB desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de HADB desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de HADB](#)

Introducción

Al actualizar HADB de Java ES Versión 4 a Java ES Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización.

- **Enfoque general de actualización.** Para realizar la actualización se deben eliminar los paquetes de HADB de Java ES Versión 4 y agregar los paquetes de Java ES Versión 5. Existen dos enfoques de actualización disponibles:
 - **Actualización en línea.** Utilice la actualización en línea para impedir la interrupción de los servicios de HADB.
 - **Actualización sin conexión.** Utilice la actualización sin conexión si puede interrumpir los servicios de HADB al sustituir los paquetes de HADB por nuevas versiones.
- **Dependencias de actualización.** HADB no presenta fuertes relaciones de dependencia. HADB requiere J2SE Versión 1.4 o posterior, lo que significa que presenta una relación leve de dependencia con J2SE.
- **Compatibilidad con versiones anteriores.** HADB incluido en Java ES Versión 5 es compatible con HADB incluido en Java ES Versión 4.
- **Anulación de la actualización.** Para deshacer la actualización desde Java ES Versión 5 a Java ES Versión 4, restaure los paquetes de las versiones de la Versión 4.
- **Problemas de plataforma.** El enfoque general de actualización de HADB es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de HADB

En esta sección se describe cómo realizar una actualización de HADB de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de HADB](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de HADB, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de HADB](#)
- [Copia de seguridad de los datos de directorio y de los archivos de configuración](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Puede verificar la versión actual de HADB mediante las utilidades estándar de comprobación de versión. Por ejemplo:

En Solaris:

```
pkgparam -v SUNWhadba
```

En Linux:

```
rpm -qi sun-hadb-a-4.4.2-7.i386.rpm
```

Tabla 9-4 Resultados de la verificación de la versión de HADB

Versión de Java ES	Número de versión de HADB
Versión 2	VERSION=4.4.0,REV=14
	SUNW_PRODVERS=4.4.0
Versión 3	VERSION=4.4.1,REV=7
	SUNW_PRODVERS=4.4.1

Tabla 9-4 Resultados de la verificación de la versión de HADB

Versión de Java ES	Número de versión de HADB
Versión 4	VERSION=4.4.2,REV=7 SUNW_PRODVERS=4.4.2
Componente de producto de la	VERSION=4.4.3,REV=5 SUNW_PRODVERS=4.4.3

Actualización de las dependencias de HADB

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Sin embargo, todos los componentes compartidos requeridos por HADB (concretamente J2SE) se actualizan automáticamente mediante el programa de instalación de Java ES cuando realice una actualización de HADB a la Versión 5.

Copia de seguridad de los datos de directorio y de los archivos de configuración

El proceso de actualización de HADB de Java ES Versión 4 a Java ES Versión 5 no modifica los datos dinámicos de HADB. No obstante, puede realizar una copia de seguridad de los paquetes de Java ES Versión 4 por si necesita deshacer la actualización.

Además, realice una copia de seguridad de los siguientes archivos, si los ha modificado desde la última instalación de HADB.

```
/etc/opt/SUNWhadb/mgt.cfg
/etc/init.d/ma-initd
```

Obtenga las contraseñas y la información de configuración necesarias

Para actualizar HADB, debe conocer la contraseña de superusuario.

Actualización de la Versión 4 de HADB

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de HADB, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de HADB a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- En función de los requisitos de producción, debe determinar qué tipo de actualización es la más adecuada: la actualización en línea o sin conexión.

- Los paquetes de actualización de Java ES Versión 5 para las plataformas Linux y Solaris se muestran en la siguiente tabla: Los paquetes de Solaris se muestran con su secuencia de instalación.

Tabla 9-5 Versiones de los paquetes de actualización de HADB en las plataformas Solaris

Paquetes de Solaris	Paquetes de Linux
SUNWhadba	sun-hadb-a-4.4.3-5.i386.rpm
SUNWhadbc	sun-hadb-c-4.4.3-5.i386.rpm
SUNWhadbe	sun-hadb-e-4.4.3-5.i386.rpm
SUNWhadbi	sun-hadb-i-4.4.3-5.i386.rpm
SUNWhadbj	sun-hadb-j-4.4.3-5.i386.rpm
SUNWhadbm	sun-hadb-m-4.4.3-5.i386.rpm
SUNWhadbs	sun-hadb-s-4.4.3-5.i386.rpm
SUNWhadbv	sun-hadb-v-4.4.3-5.i386.rpm
SUNWhadbx	sun-hadb-x-4.4.3-5.i386.rpm

Actualizaciones en línea de HADB

Al realizar una actualización en línea de HADB, debe instalar en primer lugar la Versión 5 de HADB en cada servidor del clúster que se vaya a actualizar. Cada servidor anula primero el registro de la instalación anterior de HADB y, a continuación, registra la versión recién instalada de HADB.

Para obtener información sobre cómo realizar una actualización en línea, consulte la siguiente sección de la *Sun Java System Application Server Enterprise Edition 8.2 High Availability Administration Guide*
<http://docs.sun.com/doc/819-4740/6n4r9qo7n?a=view>

Actualizaciones sin conexión de HADB

La actualización sin conexión de HADB está disponible cuando se actualiza desde Java ES Versión 3 o Versión 4.

Para realizar una actualización sin conexión, cierre los servicios de HADB y sustituya los paquetes de HADB existentes por las nuevas versiones disponibles de la distribución de Java ES 5 (Versión 5), que aparecen en la [Tabla 9-5 en la página 187](#).

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Cierre todos los servicios de HADB.

- a. Enumere todas las bases de datos que se estén ejecutando.

```
HADB-base/bin/hadbm list
```

- b. Cierre cada una de las bases de datos enumeradas.

```
HADB-base/bin/hadbm stop databaseName
```

Ignore el mensaje si alguna de las bases de datos se encuentra “detenida”.

- c. Cierre el agente de administración de HADB en cada host que lo esté ejecutando:

```
/etc/init.d/ma-initd stop
```

(La secuencia de comandos `ma-initd` se encuentra en `HADB-base/bin`, si ha instalado HADB con el programa de instalación independiente de Application Server en lugar de hacerlo con el programa de instalación de Java ES.)

3. Inicie el programa de instalación de Java ES.

```
cd Java ES Release 5 distribution/os_arch  
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, `Solaris_sparc`. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

4. Seleccione el Almacén de sesión de alta disponibilidad 4.4 en la página de selección de componentes.

Si ya ha seleccionado Application Server Enterprise Edition 8.2, entonces HADB se selecciona automáticamente.

5. Confirme el tipo de actualización que desee llevar a cabo.

Los paquetes de Application Server se actualizarán y se mostrará un resumen de la actualización.

6. Salga del programa de instalación de Java ES.

7. Restaure los archivos de los que se realizó una copia de seguridad en [“Copia de seguridad de los datos de directorio y de los archivos de configuración” en la página 186](#).

8. Compruebe que el enlace simbólico `/opt/SUNWhadb/4`, ahora señala a *HADB-base*.

Por ejemplo, para la variable predeterminada *HADB-base*:

```
ls -l /opt/SUNWhadb/4
lrwxrwxrwx 1 root other 7 Jul 7 23:18 /opt/SUNWhadb/4 ->
4.4.3-5/
```

Verificación de la actualización

Después de completar la actualización en línea, verifíquela mediante el siguiente procedimiento. Una vez que haya comprobado que la actualización se ha realizado con éxito, pueden eliminarse los antiguos paquetes de instalación.

Para verificar que los procesos en ejecución estén utilizando los servicios actualizados de HADB, puede llevar a cabo los siguientes pasos.

1. Para todos los servicios de HADB que se estén ejecutando, emita uno de los siguientes comandos:

```
HADB-base/bin/ma -V
HADB-base/bin/hadbm -V
```

Por ejemplo,

```
HADB-base/bin/ma -V
Sun Java System High Availability Database 4.4 Database Management
Agent
Versión: 4.4.3.5 [V4-5-3-5 2006-03-31 13:59:50 pakker@astra07]
(SunOS_5.9_sparc)
```

2. Compruebe si se está ejecutando la base de datos.

```
HADB-base/bin/hadbm status -n databaseName
```

Por ejemplo, para una base de datos con el nombre Example DB, introduzca los siguientes comandos.

```
HADB-base/bin/hadbm list
```

```
Base de datos
```

```
ExampleDB
```

```
HADB-base/bin/hadbm status ExampleDB
```

```
Base de datos      Estado
```

```
ExampleDB      FaultTolerant
```

```
HADB-base/bin/hadbm status -n ExampleDB
```

Núm. de nodo	Nombre de host	Puerto	Rol del
nodo	Estado del nodo	Nodo de duplic.	
0	sungod012	15000	active running 1
1	sungod012	15020	active running 0

Todos los servicios de HADB de los nodos enumerados deben presentar el estado “en ejecución”.

3. Verifique que todos los productos que utilizan HADB están usando la nueva ruta de HADB.

```
HADB-base/bin/hadbm get PackageName databaseName
```

Por ejemplo, para una base de datos con el nombre Example DB, introduzca los siguientes comandos.

```
HADB-base/bin/hadbm get PackageName ExampleDB
```

```
Atributo      Valor
```

```
PackageName V4.4.3.5
```

El comando anterior muestra la versión actual de HADB. Para obtener un listado detallado, ejecute el siguiente comando:

```
HADB-base/bin/hadbm get --all ExampleDB
```

Tareas posteriores a la actualización

No hay tareas posteriores a la actualización, más allá de las descritas en [“Actualización de HADB desde Java ES Versión 4” en la página 184.](#)

Anulación de la actualización

Para deshacer la actualización de HADB, sustituya las versiones nuevas de los paquetes de HADB que ha instalado por las versiones de las que anteriormente ha hecho copia de seguridad, como se describe en [“Copia de seguridad de los datos de directorio y de los archivos de configuración”](#) en la página 186.

Actualización de HADB desde Java ES Versión 3

El procedimiento para actualizar HADB de Java ES 2005Q1 (Versión 3) a la Versión 5 es el mismo que el que se sigue para actualizar HADB de la Versión 4 a la Versión 5.

Para actualizar HADB de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en “[Actualización de HADB desde Java ES Versión 4](#)” en la página 184 y sustituya la referencia a la Versión 4 por la Versión 3.

Message Queue

En este capítulo se describe cómo actualizar el software de Message Queue desde las versiones anteriores de Java ES a Java ES 5 (Versión 5): Sun Java System Message Queue 3.7 UR1.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Message Queue” en la página 194
- “Actualización de Message Queue desde Java ES Versión 4” en la página 199
- “Actualización de Message Queue desde Java ES Versión 3” en la página 206
- “Actualización de Message Queue desde Java ES Versión 2” en la página 207

NOTA Las ubicaciones de los archivos de este capítulo se especifican en relación con la ruta de directorio a la que se denomina *MessageQueue-base*.

El valor de *MessageQueue-base* depende de la plataforma de sistema operativo que se utilice, como se muestra en la siguiente tabla.

Tabla 10-1 Message Queue Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>MessageQueue-base</i>	/usr/bin	/opt/sun/mq/bin

Visión general de la actualización de Message Queue

En esta sección se describen los siguientes aspectos generales de Message Queue que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Message Queue de Java ES Versión 5](#)
- [Guía de actualización de Message Queue](#)
- [Datos de Message Queue](#)
- [Estrategia de actualización para Message Queue](#)

Acerca de Message Queue de Java ES Versión 5

El componente Message Queue de Java ES Versión 5 representa una actualización menor en comparación con la Versión 4. Contiene principalmente correcciones del código sin mejoras en las funciones menores.

El software de Message Queue ha incluido siempre dos ediciones, Platform Edition y Enterprise Edition; cada una de ellas se correspondía con un conjunto de características y una funcionalidad bajo licencia distintas. Enterprise Edition permitía implementar y ejecutar aplicaciones de mensajería en un entorno de producción empresarial. Platform Edition se utilizaba principalmente para desarrollar y depurar aplicaciones y componentes de mensajería, así como para probar su carga. Con la Versión 5 de Message Queue, Platform Edition ha sido rechazada y Message Queue incluye todas las funciones de Enterprise Edition. Si se realiza una actualización desde una versión anterior de Java ES a la Versión 5, cualquier edición instalada de Platform Edition se convierte en una edición con funciones completas del ámbito empresarial de Message Queue.

Guía de actualización de Message Queue

La [Tabla 10-2](#) muestra las rutas de actualización compatibles de Message Queue para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 10-2 Rutas de actualización a Java ES 5 (Versión 5): Message Queue 3.7 UR1

Versión de Java ES	Message Queue Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Message Queue 2005Q4 (3.6 SP3)) Sólo Enterprise Edition	Actualización directa: se realiza mediante el programa de instalación de Java ES.	Conversión automática de datos.
Versión 3	Sun Java System Message Queue 2005Q1 (3.6) Sólo Enterprise Edition	Actualización directa: se realiza mediante el programa de instalación de Java ES.	Conversión automática de datos.
Versión 2	Sun Java System Message Queue 2004Q2 (3.5 SP1) Platform Edition y Enterprise Edition	Actualización directa: se realiza mediante la secuencia de comandos mqupgrade.	Se realiza automáticamente en la plataforma Solaris, mientras que en Linux se utiliza la secuencia de comandos mqmigrate.
Versión 1	Sun Java System Message Queue 2003Q4 (3.0.1 SP2) Platform Edition y Enterprise Edition	Actualización directa no certificada: Aunque puede realizarse mediante la secuencia de comandos mqupgrade. ¹	Se realiza automáticamente en la plataforma Solaris, mientras que en Linux se utiliza la secuencia de comandos mqmigrate.
Versiones anteriores de Java ES	Sun Java System Message Queue 3.0.x y versiones anteriores Platform Edition y Enterprise Edition	Actualización directa no certificada: Aunque puede realizarse mediante el programa de instalación de Java ES.	

1. Antes y después de ejecutar la secuencia de comandos mqupgrade será necesario realizar copias de seguridad y, seguidamente, un restablecimiento de los siguientes archivos: por ejemplo, en el SO Solaris: restauración de /etc/imq/passwd y /etc/imq/accesscontrol.properties a /var/imq/instances/instanceName/etc/

Además de las versiones de Java ES deMessage Queue mostradas en la [Tabla 10-2](#), Message Queue también incluye el software del sistema operativo Solaris. La actualización de las versiones integradas de Message Queue a la Versión 5 se puede realizar mediante el programa de instalación de Java ES.

Datos de Message Queue

Message Queue, al igual que otros componentes Java ES, utiliza diversos tipos de datos para una actualización específica que es posible que se deban migrar a una versión actualizada. La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Message Queue.

La [Tabla 10-3](#) muestra la ubicación de los datos en los sistemas Solaris. La ubicación en los sistemas Linux es parecida (/imq en la tabla se sustituye por /opt/sun/imq). Consulte la *Message Queue 3.7 UR1 Administration Guide*, <http://docs.sun.com/doc/819-4467/6n6k98br1?a=view>.

En la [Tabla 10-3](#), *instanceName* identifica el nombre de la instancia del agente de Message Queue al que están asociados los datos.

Tabla 10-3 Message Queue Uso de datos (SO Solaris)

Categoría de datos	Ubicación (en Solaris)	Uso
Propiedades de configuración de la instancia del agente	/var/imq/instances/ <i>instanceName</i> /props/config.properties	Agente y configuraciones de servicios relacionados
Almacén persistente de datos de aplicación dinámicos	Versión 2, Versión 3 y Versión 4: /var/imq/instances/ <i>instanceName</i> /fs350/ Versión 5: /var/imq/instances/ <i>instanceName</i> /fs370/ o un almacén de datos accesible desde JDBC	Almacena mensajes, destinos, suscripciones duraderas, transacciones y otros datos dinámicos
Objetos administrados (almacén de objetos)	Directorio local de su elección o un Directory Server LDAP	Objetos utilizados para configurar las conexiones entre el cliente y el agente
Seguridad: depósitos de usuarios	/var/imq/instances/ <i>instanceName</i> /etc/passwd un servidor de directorio LDAP	Almacena los datos de usuario para la autenticación y la autorización.
Seguridad: archivo de control de acceso (ubicación predeterminada)	/var/imq/instances/ <i>instanceName</i> /etc/accesscontrol.properties	Define las reglas que autorizan el acceso del usuario a los destinos y las funciones relacionadas.
Seguridad: directorio del archivo de contraseñas (ubicación predeterminada)	/var/imq/instances/ <i>instanceName</i> /etc/	Almacena información de contraseñas cifrada.
Seguridad: ubicación del archivo del almacén de claves del agente	/etc/imq/	Almacena información de certificados cifrada para una mensajería segura.

Estrategia de actualización para Message Queue

La estrategia utilizada para la actualización de Message Queue depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1](#), “[Planificación de las actualizaciones](#)”: ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Message Queue presentando una serie de problemas que pueden influir en el plan de actualización de Message Queue.

Problemas de compatibilidad

La Versión 5 de Message Queue no introduce nuevas incompatibilidades con respecto a la Versión 3 ni a la Versión 4. Sin embargo, existen algunos problemas de compatibilidad significativos en relación con la Versión 2 y versiones anteriores. Éstos se muestran en “[Problemas de compatibilidad con la Versión 2](#)” en la [página 208](#).

Además, como regla general, si se combinan los agentes de la Versión 4 y de versiones anteriores de Message Queue con agentes de la Versión 5 de Message Queue en un clúster, el agente maestro debe pertenecer a la versión más antigua y el clúster se ejecutará como un clúster de la versión más antigua de Message Queue.

Message QueueDependencias

Las dependencias de Message Queue con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Message Queue. Por ejemplo, los cambios en las interfaces o las funciones de Message Queue pueden requerir las versiones actualizadas de los componentes de los que depende Message Queue. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Message Queue presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Message Queue presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).

- **Directory Server.** Message Queue tiene una dependencia opcional con Directory Server: puede configurar Message Queue para que se almacenen los objetos administrados o los datos de usuario en un directorio LDAP (Directory Server) en lugar de ser almacenados localmente.
- **Contenedor web.** Message Queue tiene una dependencia opcional con Web Server, Application Server o con un contenedor web de terceros para poder admitir mensajería HTTP entre el cliente y el agente.
- **Bases de datos.** Message Queue tiene una dependencia opcional con Java DB (o bases de datos de terceros) para proporcionar un almacenamiento de datos accesible desde JDBC, en lugar de un almacenamiento de mensajes de archivos simples, para la capa de persistencia de Message Queue.
- **Sun Cluster.** Message Queue tiene una dependencia opcional con Sun Cluster para proporcionar compatibilidad con alta disponibilidad.

Actualización de Message Queue desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Message Queue desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Message Queue](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Message Queue Versión 4 a la Versión 5 de Java ES, hay que tener en cuenta los siguientes aspectos del proceso de actualización:

- **Enfoque general de actualización .** La actualización se lleva a cabo mediante el programa de instalación de Java ES. El programa de instalación migra automáticamente los datos de configuración desde la Versión 4. Además, los datos de aplicación dinámicos asociados con la Versión 4 se convertirán automáticamente la primera vez que se ejecute `mqbrokerd`. En el caso de un almacén basado en archivos, esto significa que el contenido del directorio `fs350` se copiará en un directorio nuevo `fs370`. En el caso de un almacén JDBC, se producirá una actualización simple de la versión en las tablas de las bases de datos existentes.
- **Dependencias de actualización.** Message Queue presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realice una actualización de Message Queue.

Además, la Versión 5 de Message Queue presenta relaciones de dependencia con los componentes de productos de Java ES, como se describe en [“Message QueueDependencias” en la página 197](#). Sin embargo, no es necesaria la actualización de estos componentes para actualizar Message Queue a la Versión 5.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Message Queue es totalmente compatible con la Versión 4 en lo que se refiere a protocolos, compatibilidad del agente, objetos administrados, herramientas de administración y aplicaciones de cliente.

- **Anulación de la actualización.** No existe ninguna utilidad para deshacer la actualización de Message Queue a la Versión 4. Debe eliminar los componentes actualizados y restaurar manualmente la versión y los datos de configuración anteriores.
- **Problemas de plataforma.** El enfoque de actualización general de Message Queue es idéntico tanto en el sistema operativo Solaris como en Linux.

Actualización de la Versión 4 de Message Queue

En esta sección se describe cómo realizar una actualización de Message Queue de Java ES Versión 4 a Java ES Versión 5:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Message Queue](#)
- [Verificación de la actualización de Message Queue](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Message Queue, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Message Queue](#)
- [Copia de seguridad de Message Queue](#)

Verifique la información sobre la versión actual

Para determinar la versión y la edición de Message Queue instalada en el sistema, inicie el agente de Message Queue con la opción `-version`:

```
imqbrokerd -version
```

Tabla 10-4 Resultados de la verificación de la versión de Message Queue

Versión de Java ES	Número de versión de Message Queue
Versión 2	Sun Java(tm) System Message Queue 3 2004Q2 Versión: 3.5
Versión 3	Sun Java(tm) System Message Queue 3 2005Q1 Versión: 3.6
Versión 4	Sun Java(tm) System Message Queue 3 2005Q4 Versión: 3.6 SP3
Componente de producto de la	Sun Java(tm) System Message Queue 3.7 Versión: 3.7 UR1

Actualización de las dependencias de Message Queue

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Message Queue presenta fuertes relaciones de dependencia únicamente con un par de componentes compartidos.

Al actualizar las dependencias de Message Queue, debe seguir el orden que le mostramos a continuación (omitiendo cualquiera que ya se haya actualizado), antes de actualizar Message Queue. El programa de instalación de Java ES realiza automáticamente la actualización de los componentes compartidos.

- 1. Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Message Queue cuando realiza una actualización a la Versión 5 de Message Queue.
- 2. Sun Cluster (dependencia leve de actualización).** Las instrucciones para actualizar Sun Cluster a la Versión 5 están disponibles en el [Capítulo 3, “Software de Sun Cluster” en la página 81](#).
- 3. Directory Server (dependencia leve de actualización).** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [Capítulo 5, “Directory Server” en la página 107](#).
- 4. Java DB (dependencia leve de actualización).** Tiene que realizar una nueva instalación de la Versión 5 de Java DB cuando actualice Message Queue.

5. **Software de contenedor web (dependencia leve de actualización).** Las instrucciones para actualizar Web Server o Application Server están disponibles en el [Capítulo 7, “Web Server” en la página 141](#) y en el [Capítulo 11, “Application Server” en la página 219](#), respectivamente.

Copia de seguridad de Message Queue

Antes de llevar a cabo la actualización, es recomendable realizar siempre una copia de seguridad de los datos de aplicación en un entorno de producción. Tenga en cuenta la ubicación del almacén persistente de datos de aplicación dinámicos indicada en la [Tabla 10-3 en la página 196](#).

Actualización de la Versión 4 de Message Queue

El proceso de actualización consta de los siguientes pasos:

1. Detenga todas las aplicaciones de cliente de Message Queue.

Si se utiliza Message Queue en un entorno de Application Server, cierre también Application Server.
2. Detenga cualquier agente que esté en ejecución. Se le pedirá el nombre de usuario de administrador y la contraseña.

`imqcmd shutdown bkr [-b hostName:port]`
3. Si no desea conservar los datos dinámicos, el depósito de usuarios de archivos simples de Message Queue y el archivo de control de acceso de Message Queue asociado a cada instancia del agente, elimine estos datos con el siguiente comando:

`imqbrokerd -name instanceName -remove instance`

De lo contrario, se conservarán los datos dinámicos y la información de configuración para la Versión 5 de Message Queue.
4. Inicie sesión como root.

`su -`

5. Inicie el programa de instalación de Java ES.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

6. Seleccione Message Queue en la página de selección de componentes.
7. Confirme el tipo de actualización que desee llevar a cabo.

Los paquetes de Message Queue se actualizarán y se mostrará un resumen de la actualización.

8. Salga del programa de instalación de Java ES.

Verificación de la actualización de Message Queue

Una vez finalizado el proceso de actualización, compruebe que se ha realizado con éxito. Para ello, inicie el agente de Message Queue con la opción `-version`.

```
imqbrokerd -version
```

El comando devuelve el número de versión de Java ES, así como el número de versión específico de Message Queue.

Tareas posteriores a la actualización

Si ha actualizado el contenedor web y utiliza el servlet de túnel de HTTP de Message Queue, es posible que deba implementarlo otra vez en el nuevo contenedor web. No se produce ningún cambio en el servlet de túnel de HTTP entre la Versión 4 y la Versión 5. Para más información sobre compatibilidad HTTP, consulte la *Message Queue 3.7 UR1 Administration Guide*, <http://docs.sun.com/doc/819-4467>.

Si está seguro de que no tendrá que deshacer la actualización, puede eliminar de la Versión 4 los datos basados en archivo que se encuentran en el directorio `fs350` (consulte la [Tabla 10-3 en la página 196](#)).

Anulación de la actualización

No se proporciona ninguna secuencia de comandos para restablecer Message Queue al estado anterior a la actualización. Este proceso debe realizarse manualmente mediante los siguientes pasos:

1. Detenga todas las aplicaciones de cliente de Message Queue.
2. Detenga cualquier agente que esté en ejecución. Se le pedirá el nombre de usuario de administrador y la contraseña.

```
imqcmd shutdown bkr [-b hostName:port]
```

3. Si desea conservar los datos dinámicos, el depósito de usuarios de archivos simples de Message Queue y el archivo de control de acceso de Message Queue asociado a cada instancia del agente, elimine estos datos con el siguiente comando:

```
imqbrokerd -name instanceName -remove instance
```

4. Inicie sesión como root o conviértase en superusuario.

```
su -
```

5. Recupere la lista de los paquetes de Message Queue instalados con el siguiente comando:

En Solaris:

```
pkginfo | grep -i "message queue"
```

En Linux:

```
rpm -qa | grep mq
```

6. Elimine los paquetes de Message Queue con el siguiente comando:

En Solaris:

`pkgrm packageName`

donde *packageName* hace referencia a cualquiera de los paquetes de Message Queue. Para eliminar varios paquetes, separe los nombres de los paquetes mediante un espacio.

En Linux:

`rpm -e --nodeps RPMName`

donde *RPMName* hace referencia a cualquiera de los componentes rpm de Message Queue. Para eliminar varios componentes, separe los nombres de los RPM mediante un espacio.

Tenga cuidado a la hora de eliminar los paquetes de Message Queue, ya que pueden estar siendo utilizados por otros productos. El comando `pkgrm` le avisará en caso de que exista alguna dependencia con respecto a un paquete antes de proceder a su eliminación. Cuando se le solicite, confirme la eliminación escribiendo **y** (sí).

7. Escriba “q” para salir.
8. Salga del intérprete de comandos root.
9. Vuelva a instalar la Versión 4 de Message Queue.
Utilice el programa de instalación de Java ES Versión 4.
10. Restaure la copia de seguridad de los datos de la Versión 4 de Message Queue en [“Copia de seguridad de Message Queue” en la página 202](#).

La Versión 4 de Message Queue funcionará adecuadamente con la copia de seguridad de los datos antes de actualizar a la Versión 5.

Actualización de varias instancias

Para actualizar un clúster de Message Queue, en el que varios agentes interactúan para proporcionar un servicio de mensajería escalable, puede realizar una actualización por turnos en la que el clúster permanezca en línea mientras se actualizan todas las instancias de Message Queue de la Versión 4 a la Versión 5. Debe tener en cuenta las dos condiciones siguientes cuando vaya a actualizar el clúster:

- Mientras el agente permanece cerrado para la actualización, los mensajes persistentes que almacena no están disponibles hasta que se reinicie.
- El agente principal debería actualizarse en último lugar.

Por lo demás, el procedimiento es sencillo: se cierran, actualizan y reinician los agentes uno a uno hasta que se han actualizado todos.

Actualización de Message Queue desde Java ES Versión 3

El procedimiento para actualizar Message Queue de Java ES 2005Q1 (Versión 3) a la Versión 5 es el mismo que el que se sigue para actualizar Message Queue de la Versión 4 a la Versión 5.

Para actualizar Message Queue de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Message Queue desde Java ES Versión 4” en la página 199](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Actualización de Message Queue desde Java ES Versión 2

En esta sección se incluye información sobre la actualización de Message Queue desde Java ES 2004Q2 (Versión 2) a Java ES Versión 5. Además se abordan los siguientes temas:

- [Introducción](#)
- [Problemas de compatibilidad con la Versión 2](#)
- [Actualización de la Versión 2 de Message Queue](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Message Queue de Java ES Versión 2 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** La actualización se realiza mediante la secuencia de comandos `mqupgrade` que sustituye los paquetes de software anteriores por otros nuevos y migra automáticamente los datos de configuración de la Versión 2.
- **Dependencias de actualización.** Para actualizar los componentes de Java ES en un equipo desde la Versión 2, es necesario actualizar todos los demás componentes de Java ES alojados por el equipo; no se permite la actualización selectiva de componentes de Java ES de la Versión 2 a la Versión 5. Deben actualizarse especialmente todos los componentes compartidos de Java ES utilizados por Message Queue.

Además, la Versión 5 de Message Queue depende, de forma opcional, de Directory Server y Web Server (o Application Server), tal y como se describe en [“Message QueueDependencias” en la página 197](#). Si todos estos componentes están instalados en el mismo equipo, entonces tendrán que actualizarse a la Versión 5.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Message Queue no es totalmente compatible con la Versión 2, como se describe a continuación en [“Problemas de compatibilidad con la Versión 2,”](#).
- **Anulación de la actualización.** Actualmente no está permitido deshacer la actualización de la Versión 5 a la 2 (consulte [“Anulación de la actualización”](#)).

- **Problemas de plataforma.** El enfoque general de actualización de Message Queue es idéntico tanto en el sistema operativo Solaris como en Linux. No obstante, Linux requiere algunos procedimientos adicionales. Los procedimientos que se describen a continuación indican comandos, ubicaciones de archivos o procedimientos específicos para cada plataforma cuando sea pertinente.

Problemas de compatibilidad con la Versión 2

La Versión 5 de Message Queue introduce los siguientes problemas generales de compatibilidad de Message Queue en relación con la Versión 2 y con versiones anteriores.

Compatibilidad con los protocolos

Message Queue presenta una relación de dependencia con un contenedor web para proporcionar compatibilidad del protocolo HTTP entre los clientes de Message Queue y el agente. Debido a un cambio en el protocolo, al utilizar Sun Java System Web Server para proporcionar un contenedor web para la aplicación `mqhttp.war` de Message Queue, no es posible actualizar el componente Web Server sin actualizar además Message Queue (consulte [“Tareas posteriores a la actualización”](#) en la [página 203](#) y la [página 216](#)).

Compatibilidad del agente

El agente de Message Queue de la Versión 5 puede interoperar con el agente de la Versión 4, la Versión 3 o la Versión 2. Sin embargo, los cambios efectuados en las propiedades del agente y el esquema del almacén persistente con respecto a la Versión 2 pueden afectar a la compatibilidad.

La Versión 5 de Message Queue puede utilizar los datos de la Versión 4, la Versión 3 y la Versión 2, excepto en los sistemas Linux, en los que es necesario migrar primero los datos de la Versión 2 a la 5.

Al actualizar a la Versión 5 de Message Queue, tenga en cuenta lo siguiente:

- Puede utilizar archivos `config.properties` de versiones anteriores de Message Queue. También puede copiarlos en otra ubicación y consultar la configuración de las propiedades que contienen al configurar los agentes de Message Queue de la Versión 5.

- Si es necesario, todos los datos persistentes de Message Queue (mensajes, destinos o suscripciones duraderas) se convierten automáticamente en datos de la Versión 5 de Message Queue al iniciar un agente por primera vez. Por ejemplo, todos los destinos existentes se convertirán, si es preciso, en destinos de la Versión 5 de Message Queue, conservando los atributos existentes y utilizando los valores predeterminados de los nuevos atributos.
- Si se combinan los agentes de la Versión 2 de Message Queue y los agentes de la Versión 5 de Message Queue en un clúster, el agente maestro debe pertenecer a la Versión 2 de Message Queue (o a aquella que sea menos reciente) y el clúster se ejecutará como un clúster de la Versión 2 de Message Queue.

Compatibilidad de objetos administrados

Los objetos administrados de Message Queue de la Versión 5 son idénticos a los de la Versión 3 y la Versión 4. Sin embargo, se ha cambiado el nombre de algunos objetos administrados de la Versión 3 o se han mejorado con nuevos atributos con respecto a las versiones anteriores. Por lo tanto, al actualizar Message Queue de la Versión 2 a la Versión 5, debería tener en cuenta lo siguiente:

- Puede utilizar el mismo almacén de objetos y los mismos objetos administrados que se crearon en la Versión 2, aunque es recomendable migrar los objetos administrados a la Versión 5. La consola de administración (imqadmin) y la utilidad de línea de comandos de ObjectManager (imqobjmgr) convertirán los objetos administrados de la Versión 2 a la Versión 5 al realizar una operación de actualización.
- El tiempo de ejecución de cliente de la Versión 5 buscará los objetos administrados de la Versión 2 y creará una instancia para ellos y, a continuación, los convertirá para que puedan ser utilizados por los clientes de la Versión 5. Sin embargo, esta acción *no* convertirá los objetos administrados de la Versión 2 que se encuentren en el almacén de objetos desde el que se realizó la búsqueda.
- Los clientes existentes de la Versión 2 (aplicaciones o componentes), es decir, los clientes que crean directamente instancias para los objetos administrados en lugar de buscarlos, son compatibles con la Versión 5. No obstante, si van a utilizar atributos *nuevos* de objetos administrados (consulte el capítulo 16 de la *Message Queue 3.7 UR1 Administration Guide* , <http://docs.sun.com/doc/819-4467> para obtener información sobre los atributos de objetos administrados), éstos deberán reescribirse. (Al volver a compilar los clientes de la Versión 2 con los de la Versión 5, se mostrarán los atributos de la Versión 2 de Message Queue que han cambiado de nombre en la Versión 5. Los nombres antiguos seguirán funcionando.)

- Las secuencias de comandos que inician clientes de Java y establecen los valores de los atributos de objetos administrados mediante las opciones de la línea de comandos son compatibles con la Versión 5. No obstante, si utilizan atributos *nuevos* de objetos administrados (consulte el capítulo 16 de la *Message Queue 3.7 UR1 Administration Guide*, <http://docs.sun.com/doc/819-4467> para obtener información sobre los atributos de objetos administrados), éstos deberán reescribirse.

Compatibilidad de herramientas de administración

Debido a la adición de nuevos comandos y nuevas funciones administrativas en la Versión 3, las herramientas administrativas de la Versión 5 (la consola de administración y las utilidades de línea de comandos) sólo funcionan con los agentes de las Versiones 3, 4 y 5. No obstante, se siguen admitiendo todos los comandos y las opciones de comando de la Versión 2.

Compatibilidad de clientes

Los clientes de la Versión 3 y la Versión 4 son completamente compatibles con la Versión 5 de Message Queue. Sin embargo, al actualizar de la Versión 2 a la Versión 5, debería tener en cuenta los siguientes problemas de compatibilidad relacionados con los clientes de Java:

- Un agente de la Versión 5 es compatible con un cliente de la Versión 2 (pero sin las funciones adicionales de la Versión 5).
- Un cliente de la Versión 5 de Java se puede conectar a un agente de la Versión 2 (pero sin las funciones adicionales de la Versión 5).
- Los programas de cliente C sólo son compatibles con los agentes de la Versión 5 y de la Versión 2, 3 ó 4 que se ejecutan con una licencia de prueba de Platform Edition o una licencia de Enterprise Edition.

Actualización de la Versión 2 de Message Queue

En esta sección se describe cómo realizar una actualización de Message Queue de Java ES Versión 2 a Java ES Versión 5:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 2 de Message Queue \(Solaris\)](#)
- [Actualización de la Versión 2 de Message Queue \(Linux\)](#)

- [Instalación del paquete de compatibilidad \(Linux\)](#)
- [Verificación de la actualización de Message Queue](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Message Queue, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Message Queue](#)
- [Copia de seguridad de Message Queue](#)

Verifique la información sobre la versión actual

Para determinar la versión y la edición de Message Queue instalada en el sistema, inicie el agente de Message Queue con la opción `-version`:

```
imqbrokerd -version
```

Tabla 10-5 Resultados de la verificación de la versión de Message Queue

Versión de Java ES	Número de versión de Message Queue
Versión 2	Sun Java(tm) System Message Queue 3 2004Q2 Versión: 3.5
Versión 3	Sun Java(tm) System Message Queue 3 2005Q1 Versión: 3.6
Versión 4	Sun Java(tm) System Message Queue 3 2005Q4 Versión: 3.6 SP3
Componente de producto de la	Sun Java(tm) System Message Queue 3.7 Versión: 3.7 UR1

Actualización de las dependencias de Message Queue

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Message Queue presenta fuertes relaciones de dependencia únicamente con un par de componentes compartidos.

Al actualizar las dependencias de Message Queue, debe seguir el orden que le mostramos a continuación (omitiendo cualquiera que ya se haya actualizado), antes de actualizar Message Queue.

1. **Componentes compartidos.** Las instrucciones para actualizar los componentes compartidos de Java ES a la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#)).
2. **Sun Cluster (dependencia leve de actualización).** Las instrucciones para actualizar Sun Cluster a la Versión 5 están disponibles en el [Capítulo 3, “Software de Sun Cluster” en la página 81](#).
3. **Directory Server (dependencia leve de actualización).** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [Capítulo 5, “Directory Server” en la página 107](#).
4. **Java DB (dependencia leve de actualización).** Tiene que realizar una nueva instalación de la Versión 5 de Java DB cuando actualice Message Queue.
5. **Software de contenedor web (dependencia leve de actualización).** Las instrucciones para actualizar Web Server o Application Server están disponibles en el [Capítulo 7, “Web Server” en la página 141](#) y en el [Capítulo 11, “Application Server” en la página 219](#), respectivamente.

Copia de seguridad de Message Queue

Antes de llevar a cabo la actualización, es recomendable realizar siempre una copia de seguridad de los datos de aplicación en un entorno de producción. En la plataforma del SO Solaris, los datos dinámicos se almacenan en el directorio siguiente:

`/var/imq/instances/instanceName.`

Para obtener información sobre otros sistemas operativos, consulte la *Message Queue 3.7 UR1 Administration Guide*, <http://docs.sun.com/doc/819-4467>.

Actualización de la Versión 2 de Message Queue (Solaris)

La actualización del software de Message Queue a Java ES Versión 5 utiliza la secuencia de comandos `mqupgrade` para instalar los paquetes de la Versión 5.

El proceso de actualización consta de los siguientes pasos:

1. Detenga todas las aplicaciones de cliente de Message Queue.

Si se utiliza Message Queue en un entorno de Application Server, cierre también Application Server.

2. Detenga cualquier agente que esté en ejecución. Se le pedirá el nombre de usuario de administrador y la contraseña.

```
imqcmd shutdown bkr [-b hostName:port]
```

3. Si no desea conservar los datos dinámicos, el depósito de usuarios de archivos simples de Message Queue y el archivo de control de acceso de Message Queue asociado a cada instancia del agente, elimine estos datos con el siguiente comando:

```
imqbrokerd -name instanceName -remove instance
```

De lo contrario, se conservarán los datos dinámicos y la información de configuración para la Versión 5 de Message Queue.

4. Inicie sesión como root.

```
su -
```

5. Cambie los directorios a la ubicación del directorio Tools de la distribución de Java ES Versión 5.

En Solaris SPARC:

```
cd Solaris_sparc/Product/message_queue/Tools
```

En Solaris x86:

```
cd Solaris_x86/Product/message_queue/Tools
```

6. Ejecute la secuencia de comandos mqupgrade .

- a. Inicie la secuencia de comandos:

```
./mqupgrade
```

La secuencia de comandos mqupgrade muestra los componentes instalados en Message Queue.

- b. Introduzca y (sí) para actualizar los componentes de Message Queue.

La secuencia de comandos mqupgrade detecta y muestra los archivos de traducción.

Si no desea actualizar los componentes de Message Queue, introduzca n (no). La secuencia de comandos mqupgrade saldrá sin actualizar los componentes de Message Queue.

- c. Si se le solicita, introduzca y (sí) para actualizar los archivos de traducción.

La secuencia de comandos `mqupgrade` envía el resultado a un archivo de registro en la siguiente ubicación:

```
/var/sadm/install/logs/Message_Queue_upgrade_'date'.log
```

Actualización de la Versión 2 de Message Queue (Linux)

La actualización de Message Queue de la Versión 2 a la Versión 5 en la plataforma Linux se complica por el hecho de que Java ES Versión 2 sólo se admite en RHEL 2.1, pero Java ES Versión 5 no se admite en RHEL 2.1. Por lo tanto, es necesaria una actualización doble: deben actualizarse tanto el sistema operativo como Message Queue. Consulte [“Actualizaciones dobles: El software de Java ES y el sistema operativo” en la página 46](#).

El procedimiento básico es actualizar primero el sistema operativo Linux, a continuación todas las dependencias de Message Queue y, por último, Message Queue.

La actualización de Message Queue de la Versión 2 a la Versión 5 incluye un paso de migración de datos que no es necesario en el caso de los sistemas Solaris; se trata, concretamente, de la migración de datos de la instancia del agente a la ubicación apropiada de la Versión 5. Si desea conservar los datos de la Versión 2 al actualizar a la Versión 5, Message Queue proporciona una herramienta, `mqmigrate`, para realizar esta migración.

Para actualizar de la Versión 2 a la Versión 5, siga las mismas instrucciones que aparecen en [“Actualización de la Versión 2 de Message Queue \(Solaris\)” en la página 212](#) y ejecute la secuencia de comandos `mqmigrate` ([Paso 6 en la página 215](#)) antes de ejecutar la secuencia de comandos `mqupgrade` ([Paso 7 en la página 215](#)), como se detalla en el siguiente procedimiento.

1. Detenga todas las aplicaciones de cliente de Message Queue.
2. Detenga cualquier agente que esté en ejecución. Se le pedirá el nombre de usuario de administrador y la contraseña.

```
imqcmd shutdown bkr [-b hostName:port]
```

3. Si no desea conservar los datos dinámicos, el depósito de usuarios de archivos simples de Message Queue y el archivo de control de acceso de Message Queue asociado a cada instancia del agente, elimine estos datos con el siguiente comando:

```
imqbrokerd -name instanceName -remove instance
```

De lo contrario, se conservarán los datos dinámicos y la información de configuración para la Versión 5 de Message Queue.

4. Inicie sesión como root o conviértase en superusuario.

```
su -
```

5. Cambie los directorios a la ubicación del directorio Tools de la distribución de Java ES Versión 5.

```
cd Linux_x86/Product/message_queue/Tools
```

6. Migre los datos de la instancia del agente con el siguiente comando:

```
./mqmigrate
```

La secuencia de comandos `mqmigrate` transferirá los datos de configuración de la instancia del agente de la Versión 2 a la ubicación adecuada R4.

7. Ejecute la secuencia de comandos `mqupgrade`.

- a. Inicie la secuencia de comandos:

```
./mqupgrade
```

La secuencia de comandos `mqupgrade` muestra los componentes instalados en Message Queue.

- b. Introduzca y (sí) para actualizar los componentes de Message Queue.

La secuencia de comandos `mqupgrade` detecta y muestra los archivos de traducción.

Si no desea actualizar los componentes de Message Queue, introduzca n (no). La secuencia de comandos `mqupgrade` saldrá sin actualizar los componentes de Message Queue.

- c. Si se le solicita, introduzca y (sí) para actualizar los archivos de traducción.

La secuencia de comandos `mqupgrade` envía el resultado a un archivo de registro en la siguiente ubicación:

```
/var/sadm/install/logs/Message_Queue_upgrade_'date'.log
```

Instalación del paquete de compatibilidad (Linux)

Si tiene secuencias de comandos de la Versión 2, o las aplicaciones de cliente contienen secuencias de comandos de dicha versión que dependen de la ubicación de los archivos instalados de la Versión 5, deberá instalar el paquete `sun-mq-compat`, que contiene enlaces simbólicos desde las ubicaciones de los archivos de la Versión 2 a las de la Versión 5.

El paquete `sun-mq-compat` se encuentra en la siguiente ubicación en la que se descomprimió la distribución de Java ES Versión 5.

`Linux_x86/Product/message_queue/Packages`

Lleve a cabo los siguientes pasos para instalar el paquete `sun-mq-compat`:

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. En el directorio de paquetes, introduzca el siguiente comando:

`rpm -ivh --nodeps sun-mq-compat-3.7-RelNo.i386.rpm`

Verificación de la actualización de Message Queue

Una vez finalizado el proceso de actualización, compruebe que se ha realizado con éxito. Para ello, inicie el agente de Message Queue con la opción `-version`.

`imqbrokerd -version`

El comando devuelve el número de versión de Java ES, así como el número de versión específico de Message Queue.

Tareas posteriores a la actualización

Si utiliza el servlet de túnel de HTTP para proporcionar compatibilidad con el servicio de conexión HTTP, este servlet se actualizará cuando se actualice Message Queue de la Versión 2 a la Versión 5. Para ello, es necesario volver a implementarlo una vez realizada la actualización de Message Queue a la Versión 5. Consulte la *Message Queue Administration Guide*, (<http://docs.sun.com/doc/819-4467>) para obtener más información sobre la compatibilidad con HTTP.

Migre los objetos administrados de la Versión 2 a las versiones de la Versión 5 mediante la consola de administración (`imqadmin`) o la utilidad de línea de comandos de ObjectManager (`imqobjmgr`) para realizar una operación de actualización.

Anulación de la actualización

No se permite actualmente deshacer la actualización de Message Queue de la Versión 2 a la Versión 5. Por lo general, el procedimiento para deshacer la actualización es similar al aplicado de la Versión 5 a la Versión 4 (consulte [“Anulación de la actualización” en la página 204](#)). Sin embargo, ya que la actualización de Message Queue de la Versión 2 a la Versión 5 no actualiza el registro de producto de Java ES, el programa de instalación de Java ES no puede volver a instalar la Versión 2 de Message Queue.

Para obtener información sobre soluciones temporales a este problema, consulte Sun Services.

Actualización de varias instancias

Para actualizar un clúster de Message Queue, en el que varios agentes interactúan para proporcionar un servicio de mensajería escalable, puede realizar una actualización por turnos en la que el clúster permanezca en línea mientras se actualizan todas las instancias de Message Queue de la Versión 2 a la Versión 5. Debe tener en cuenta las dos condiciones siguientes cuando vaya a actualizar el clúster:

- Mientras el agente permanece cerrado para la actualización, los mensajes persistentes que almacena no están disponibles hasta que se reinicie.
- El agente principal debería actualizarse en último lugar.

Por lo demás, el procedimiento es sencillo: se cierran, actualizan y reinician los agentes uno a uno hasta que se han actualizado todos.

Application Server

En este capítulo se describe cómo actualizar Application Server a Java ES 5 (Versión 5): Sun Java System Application Server Enterprise Edition 8.2.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Application Server” en la página 221
- “Actualización de Application Server desde Java ES Versión 4” en la página 227
- “Actualización de Application Server desde Java ES Versión 3” en la página 234
- “Actualización de Application Server desde Java ES Versión 2” en la página 235
- “Actualización de Application Server integrado en Solaris en un entorno de zonas múltiples de Solaris 10” en la página 246

NOTA Las ubicaciones de los archivos de este capítulo se especifican en relación con las rutas de directorio a las que se denomina *AppServer8-base*, *AppServer8Config-base* (Application Server 8.x), *AppServer7-base* y *AppServer7Config-base* (Application Server 7.x). Debe haberse especificado, al menos, parte de estas rutas como directorio de instalación o de dominio durante la instalación de Application Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado. Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.

Tabla 11-1 Application Server Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>AppServer8-base</i>	/opt/SUNWappserver/appserver	/opt/sun/appserver
<i>AppServer8Install-base</i>	/opt/SUNWappserver	/opt/sun/appserver
<i>AppServer8Config-base</i>	/var/opt/SUNWappserver	/var/opt/sun/appserver
<i>AppServer7-base</i>	/opt/SUNWappserver7	/opt/SUNWappserver7
<i>AppServer7Config-base</i>	/var/opt/SUNWappserver7	/var/opt/SUNWappserver7

NOTA El nombre de dominio predeterminado de Application Server para la Versión 5 de Application Server (8.x) es `domain1`. En otras palabras, `domain1` es el valor predeterminado de la variable `domainName` utilizada en este capítulo.

Además, el nombre de la instancia predeterminada de Directory Administration Service (DAS) es `server`. Las aplicaciones de J2EE no se implementan normalmente en la instancia DAS, sino en otras instancias independientes.

Para más información acerca de los comandos `asadmin` utilizados en este capítulo, consulte el *Sun Java System Application Server Enterprise Edition 8.2 Reference Manual*, <http://docs.sun.com/doc/819-4736>.

Visión general de la actualización de Application Server

En esta sección se describen los siguientes aspectos generales de Application Server que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Application Server de Java ES Versión 5](#)
- [Guía de actualización de Application Server](#)
- [Datos de Application Server](#)
- [Estrategia de actualización para Application Server](#)

Acerca de Application Server de Java ES Versión 5

Application Server de Java ES Versión 5 representa una versión inferior en relación a la Versión 4, incluyendo sólo determinadas soluciones de errores. Aunque funcionalmente la Versión 5 de Application Server es idéntica a la Versión 4.

Guía de actualización de Application Server

Hay dos conjuntos de rutas de actualización que se pueden aplicar en la actualización de Application Server a Java ES Versión 5:

- La [Tabla 11-2](#) muestra las rutas de actualización compatibles de Application Server de Java ES a Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.
- La [Tabla 11-3](#) muestra las rutas de actualización compatibles de Application Server integrado en Solaris a Java ES Versión 5. Application Server Platform Edition está integrado en el software del sistema operativo Solaris. La actualización de las versiones integradas de Application Server a la Versión 5 de Enterprise Edition se puede llevar a cabo mediante el programa de instalación de Java ES, tal y como se indica en la [Tabla 11-3](#).

Tabla 11-2 Rutas de actualización a Java ES 5 (Versión 5): Application Server Enterprise Edition 8.2

Versión de Java ES	Application Server Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Application Server Enterprise Edition 8.1 2005Q4	Actualización directa: Se realiza mediante el programa de instalación de Java ES. ¹	Ninguna
Versión 3	Sun Java System Application Server Enterprise Edition 8.1 2005Q1	Actualización directa: se realiza mediante el programa de instalación de Java ES.	Ninguna
Versión 2	Sun Java System Application Server 7.0 Update 3 (2004Q2) Platform Edition y Enterprise Edition	Actualización directa: Utilice el programa de instalación de Java ES para actualizar los paquetes, la secuencia de comandos postInstall para llevar a cabo una reconfiguración y la utilidad asupgrade para migrar la información de dominio. ²	Variables de entorno, dominios y otros datos de configuración. Deben migrarse las aplicaciones y los componentes de J2EE al nuevo entorno de Application Server e implementarse de nuevo.
Versión 1	Sun ONE Application Server 7.0 Update 1 (2003Q4) Platform Edition y Enterprise Edition	Actualización directa no certificada: Utilice el mismo enfoque que en la actualización de Application Server desde la Versión 2.	Variables de entorno, dominios y otros datos de configuración. Deben migrarse las aplicaciones y los componentes de J2EE al nuevo entorno de Application Server e implementarse de nuevo.
Versiones anteriores de Java ES		Sin actualización directa: Aunque puede actualizar primero a la Versión 3 utilizando los procedimientos descritos en la <i>Guía de migración y actualización de Java Enterprise System 2005Q1</i> , http://docs.sun.com/doc/819-0062 . A continuación, actualice de la Versión 3 a la Versión 5.	

1. Si desea actualizar Application Server desde la Versión 4 a la Versión 5 sin que se conserve la información de configuración o de dominio, puede utilizar el programa de desinstalación de Java ES Versión 4 para desinstalar la Versión 4 de Application Server y, a continuación, utilizar el programa de instalación de Java ES Versión 5 para realizar una nueva instalación de la Versión 5 de Application Server. Sin embargo, si se ha instalado la Versión 4 de Application Server con la opción Configurar más tarde, entonces, antes de desinstalar la Versión 4 de Application Server debe crear un archivo `$HOME/.asadminprefs` (donde `$HOME` es el directorio de inicio para el usuario que instala y ejecuta Application Server). El archivo tiene las dos líneas siguientes:
`AS_ADMIN_PASSWORD=password`
`AS_ADMIN_USER=admin`

2. Deberá prestar una atención especial cuando vaya a realizar una actualización desde la Versión 2 de Application Server en una plataforma de Solaris, puesto que tanto Application Server integrado en Solaris, como Application Server de Java ES Versión 2 coexisten en el equipo. Consulte la [Tabla 11-3](#) y la nota que se incluye al final de dicha tabla.

Tabla 11-3 Rutas de actualización para las versiones integradas de Application Server con el sistema operativo Solaris

Versión del SO Solaris	Application Server Versión	Enfoque general	Reconfiguración necesaria
Solaris 10	Sun Java System Application Server Platform Edition 8.0.0_01	Actualización directa: se realiza mediante el programa de instalación de Java ES.	None (Ninguna).
Solaris 9	Sun Java System Application Server 7.0.0_03c	Actualización directa: <i>Si se ha utilizado</i> Application Server y se han creado dominios, entonces la información de dominio tiene que migrarse. Utilice el enfoque que se describe en la actualización de Application Server desde la Versión 2, en la que se utiliza la opción del programa de instalación de Java ES Configurar más tarde, la secuencia de comandos postInstall y la utilidad asupgrade. <i>Si no se ha utilizado</i> Application Server o se ha utilizado pero sin crear dominios, utilice el enfoque que se describe en la actualización de Application Server desde la Versión 2 y utilice la opción Configurar más tarde del programa de instalación de Java ES; pero no utilice la secuencia de comandos postInstall ni la utilidad asupgrade.	Variables de entorno, dominios (si se han creado) y otros datos de configuración. Deben migrarse las aplicaciones y los componentes de J2EE al nuevo entorno de Application Server e implementarse de nuevo.

NOTA

Deberá prestar una atención especial cuando vaya a realizar una actualización desde la Versión 2 de Application Server en una plataforma de Solaris, puesto que tanto la versión integrada como la versión de Application Server de Java ES coexisten en el equipo. Por lo tanto, deberá desinstalar primero la versión integrada (y los dominios correspondientes) antes de llevar a cabo la actualización desde la Versión 2. Consulte el [“Sólo para Solaris: Elimine manualmente los paquetes de Application Server integrados con el sistema operativo”](#) en la página 237.

Datos de Application Server

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Application Server.

Tabla 11-4 Uso de datos de Application Server

Tipo de datos	Ubicación	Uso
Variables de entorno	<i>AppServer8-base/config/asenv.conf</i>	Variables globales
Datos de configuración	Versiones 3, 4 y 5:Archivos domain.xml y server.policy en <i>AppServer8Config-base/domains/domainName/config</i> Versión 2:Archivos server.xml y server.policy en <i>AppServer7Config-base/domains/domainName/ instanceName/config</i>	Configuración de instancias de Application Server
Datos de implementación	Versiones 3, 4 y 5: <i>AppServer8Config-base/domains/domainName/ applications</i> Versión 2: <i>AppServer7Config-base/domains/domainName/ instanceName/applications</i>	Configuración del contenedor de J2EE para aplicaciones y componentes de J2EE específicos
Acceso a archivos de registro	Versiones 3, 4 y 5: <i>AppServer8Config-base/domains/domainName/ logs/access/</i> Contiene dos archivos: server_acces_log y _asadmin_access_log Versión 2: <i>AppServer7Config-base/domains/domainName/ instanceName/logs/access</i>	Registro de acceso

Estrategia de actualización para Application Server

La estrategia utilizada para la actualización de Application Server depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Application Server presentando una serie de problemas que pueden influir en el plan de actualización de Application Server.

Problemas de compatibilidad

La Versión 5 de Application Server no presenta ningún cambio en la interfaz con respecto a la Versión 4 ni a la Versión 3. Sin embargo, existen importantes cambios entre las interfaces de la Versión 5 y la Versión 2 que hacen que estas dos versiones sean incompatibles.

No obstante, la Versión 5 de Application Server es incompatible con la Versión 4 de Service Registry. Si se actualiza Application Server a la Versión 5, también se debe actualizar Service Registry a dicha versión.

Dependencias de Application Server

Las dependencias de Application Server con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Application Server. Por ejemplo, los cambios en las interfaces y las funciones de Application Server pueden requerir las versiones actualizadas de los componentes de los que depende Application Server. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Application Server presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Application Server presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Message Queue.** Application Server depende de Message Queue para permitir el uso de la mensajería asíncrona compatible con J2EE Java Message Service.

- **Almacén de sesión de alta disponibilidad.** Application Server depende del Almacén de sesión de alta disponibilidad (HADB) para mantener la información de estado de sesión necesaria para admitir la conmutación por error entre las instancias.

NOTA	Si tiene una instalación anterior de Application Server que no requiere HADB, éste debe instalarse antes de que actualice Application Server a la Versión 5. Por ejemplo, la Versión 5 de HADB debe estar instalada para poder actualizar las versiones de Application Server integradas con el sistema operativo Solaris. El programa de instalación de Java ES realizará automáticamente la instalación de HADB en estas situaciones.
-------------	---

- **Java Database.** Application Server depende de Java Database como base de datos predeterminada del programador y para almacenar datos de aplicaciones de ejemplo así como los datos necesarios para los temporizadores de Enterprise Java Beans.
- **Contenedor web (dependencia opcional).** Application Server depende de los servicios de contenedor web para el complemento de equilibrado de carga opcional. Tanto Java ES Web Server como un contenedor de terceros (por ejemplo, Apache Web Server y Microsoft IIS) pueden ofrecer este tipo de compatibilidad.

Actualización de Application Server desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Application Server desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Application Server](#)

Introducción

Al actualizar Application Server de Java ES de la Versión 4 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización .** La actualización se lleva a cabo mediante el programa de instalación de Java ES. No es necesaria una reconfiguración de Application Server, ni tampoco una reconfiguración ni una migración de los componentes J2EE para actualizar Application Server de la Versión 4 a la Versión 5.
- **Dependencias de la actualización.** Application Server presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realiza una actualización de Application Server. Application Server presenta únicamente fuertes relaciones de dependencia con el componente compartido NSS.

Además, como se describe en [“Dependencias de Application Server” en la página 225](#), la Versión 5 de Application Server presenta relaciones de dependencia con Message Queue, HADB y Java DB. Todas estas son dependencias fuertes de actualización, por lo que todos estos componentes tienen que actualizarse a la Versión 5.

Además, Application Server depende, de forma opcional, de Java ES Web Server o de contenedores web de terceros. Sin embargo, estas dependencias de actualización son leves y la actualización del contenedor web es opcional en relación con la actualización de Application Server a la Versión 5.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Application Server es compatible con la Versión 4.

- **Anulación de la actualización.** No se puede deshacer la actualización de la Versión 4 a la Versión 5.
- **Problemas de plataforma.** El enfoque general de actualización de Application Server es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de Application Server

En esta sección se describe cómo realizar una actualización de Application Server de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Application Server](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar el software de Application Server, debe realizar las tareas descritas a continuación:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Application Server](#)
- [Copia de seguridad de los datos de Application Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Application Server, introduzca el siguiente comando:

```
AppServer8-base/bin/asadmin version --verbose
```

Tabla 11-5 Resultados de la verificación de la versión de Application Server

Versión de Java ES	Número de versión de Application Server
Versión 2	Sun ONE Application Server 7.0.0_03c
Versión 3	Sun Java Enterprise System Application Server Enterprise Edition 8.1
Versión 4	Sun Java Enterprise System Application Server Enterprise Edition 8.1_02
Componente de producto de la	Sun Java Enterprise System Application Server Enterprise Edition 8.2

Actualización de las dependencias de Application Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Application Server presenta fuertes relaciones de dependencia con el componente compartido NSS y con los componentes de los productos Message Queue, HADB y Java DB.

Al actualizar las dependencias de Application Server, debe seguir el orden que le mostramos a continuación (omitiendo cualquiera que ya se haya actualizado), antes de actualizar Application Server. Sin embargo, al actualizar Application Server con el programa de instalación de Java ES se suelen actualizar automáticamente tanto los componentes compartidos, como Message Queue, HADB y Java DB.

- 1. Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Application Server cuando realiza una actualización a la Versión 5 de Application Server.
- 2. Message Queue.** Las instrucciones para actualizar Message Queue a la Versión 5 están disponibles en el [Capítulo 10, “Message Queue” en la página 193](#).
- 3. Almacén de sesión de alta disponibilidad (HADB).** Las instrucciones para actualizar HADB están disponibles en el [Capítulo 9, “Almacén de sesión de alta disponibilidad” en la página 179](#).
- 4. Java DB.** Las instrucciones para actualizar Java DB están disponibles en el [Capítulo 8, “Java DB” en la página 171](#).

- 5. Software de contenedor web (dependencia leve de actualización).** Las instrucciones para actualizar Web Server están disponibles en el [Capítulo 7, “Web Server” en la página 141](#).

Copia de seguridad de los datos de Application Server

Al actualizar Application Server de la Versión 4 a la Versión 5, no se modifican los datos de configuración, por lo que no es necesario que realice una copia de seguridad de los datos actuales.

Obtenga las contraseñas y la información de configuración necesarias

Debe conocer el Id. de usuario y la contraseña del administrador de la versión de Application Server actualmente instalada.

Actualización de la Versión 4 de Application Server

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Application Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de Application Server a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Deben cerrarse todos los componentes de J2EE que se estén ejecutando en una instancia de Application Server antes de actualizar dicha instancia. No obstante, este requisito no es imprescindible si el equilibrado de carga proporciona alta disponibilidad o escalabilidad.
- Deben cerrarse todas las instancias de Application Server que se estén ejecutando en un único equipo (todas las que correspondan a la misma imagen instalada de Application Server) mientras se actualiza la imagen instalada.
- En las implementaciones con varios nodos, realice el procedimiento de actualización en cada nodo o en cada equipo que aloje instancias de Application Server.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia a las instancias de Application Server que residen localmente en el equipo en el que se vaya a realizar la actualización.

- 1. Inicie sesión como root o conviértase en superusuario.**

SU -

2. Cierre todos los componentes de J2EE que dependan de las instancias de Application Server que se van a actualizar.
3. Cierre todas las instancias de Application Server en el equipo que se vaya a actualizar.

- a. Detenga todos los nodos de agente que se estén ejecutando.

```
AppServer8-base/bin/asadmin stop-node-agent --user admin_ID
nodeagentName
```

donde *nodeagentName* tiene el formato *hostName_domainName*, , pero la variable predeterminada es simplemente *hostName*.

- b. Detenga Domain Administration Server (DAS).

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
domainName
```

- c. Detenga el servidor de la base de datos de PointBase, si se estuviera utilizando.

```
AppServer8Config-base/appserver/pointbase/tools/stopserver.sh
```

4. Inicie el programa de instalación de Java ES.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción *installer -nodisplay* para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

5. Seleccione Application Server en la página de selección de componentes.

Ya que Message Queue, HADB y Java DB presentan fuertes relaciones de dependencia, se seleccionarán automáticamente para la actualización.

6. Seleccione Configurar ahora.

7. Especifique los valores de configuración solicitados.

Aparecerán una serie de paneles de configuración.

8. Confirme el tipo de actualización que desee llevar a cabo.

Los paquetes de Application Server (y si fuera necesario los de Message Queue, HADB y Java DB) se actualizarán y se mostrará un resumen de la actualización.

9. Salga del programa de instalación de Java ES.
10. Reinicie el Domain Administration Server (DAS) actualizado.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

11. Reinicie las instancias actualizadas de Application Server.

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
nodeagentName
```

donde *nodeagentName* presenta el formato *hostName_domainName*, pero es sólo de forma predeterminada *hostName*.

Verificación de la actualización

Para comprobar que la actualización se ha realizado correctamente, utilice el siguiente comando:

```
AppServer8-base/bin/asadmin version --verbose
```

Consulte la [Tabla 11-5 en la página 229](#) para obtener los valores de salida.

Tareas posteriores a la actualización

Si quiere seguir utilizando la base de datos incorporada de PointBase de la Versión 4 en lugar de Java DB, un nuevo componente de producto de la Versión 5 de Java ES, deberá editar manualmente el archivo actualizado *AppServer8-base/config/asenv.conf*.

Una vez haya actualizado Application Server desde la Versión 4, los valores de configuración de PointBase en *asenv.conf* son los siguientes:

```
AS_POINTBASE="%POINTBASE_HOME%"
AS_POINTBASE_SAMPLESDB="%POINTBASE_SAMPLESDB%"
```

Cambie estos valores de configuración por los siguientes:

```
AS_POINTBASE="AppServer8-base/pointbase"
AS_POINTBASE_SAMPLESDB="AppServerConfig8-base/var/appserver/pointbase"
```

Anulación de la actualización

No se puede deshacer la actualización de la Versión 5.

Actualización de Application Server desde Java ES Versión 3

El procedimiento para actualizar Application Server de Java ES 2005Q1 (Versión 3) a la Versión 5 es el mismo que el que se emplea para actualizar Application Server de la Versión 4 a la Versión 5.

Para actualizar Application Server de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Application Server desde Java ES Versión 4” en la página 227](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Actualización de Application Server desde Java ES Versión 2

En esta sección se incluye información sobre la actualización de Application Server desde Java ES Versión 2 a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 2 de Application Server](#)

Introducción

Al actualizar Application Server de Java ES Versión 2 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque de actualización general.** Para realizar la actualización se debe instalar la Versión 5 de Application Server mediante el programa de instalación de Java ES y seleccionar la opción Configurar más tarde. Para volver a efectuar la configuración, se debe emplear la utilidad asupgrade. Una vez actualizado Application Server, se deben migrar las aplicaciones y los componentes de J2EE de la Versión 2 a la Versión 5.
- **Dependencias de actualización.** Para actualizar los componentes de Java ES en un equipo desde la Versión 2, es necesario actualizar todos los demás componentes de Java ES alojados por el equipo; no se permite la actualización selectiva de componentes de Java ES de la Versión 2 a la Versión 5.

Deben actualizarse especialmente todos los componentes compartidos de Java ES requeridos por Application Server. Si Message Queue reside en el mismo equipo, también tendrá que actualizarse. El Almacén de sesión de alta disponibilidad (HADB) y Java DB deben instalarse y, si se está utilizando Web Server como equilibrador de carga, también debe actualizarse.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Application Server no es compatible con la Versión 2. Deben migrarse las aplicaciones y los componentes de J2EE para que ejecuten en el entorno de la Versión 5 de Application Server.
- **Anulación de la actualización.** Para deshacer la actualización de la Versión 2 a la 5, sólo hay que restablecer la instalación de la Versión 2 (el proceso de actualización no elimina los datos de configuración de la Versión 2).

- **Problemas de plataforma.** El enfoque de actualización de Application Server en el sistema operativo Solaris no se puede aplicar directamente en el sistema operativo Linux. La Versión 2 de Java ES sólo se admite en Linux 2.1, mientras que la Versión 5 de Java ES no es admitida en Linux 2.1. Por lo tanto, es necesaria una doble actualización: deben actualizarse tanto el sistema operativo como Application Server (consulte [“Actualizaciones dobles: El software de Java ES y el sistema operativo” en la página 46](#))
- **Ubicaciones de datos.** En la Versión 5 hay ubicaciones nuevas de los datos de configuración, los datos de implementación y los archivos de registro de acceso, tal y como se especifica en la [Tabla 11-4 en la página 224](#).

Actualización de la Versión 2 de Application Server

En esta sección se describe cómo realizar una actualización de Application Server desde Java ES Versión 2 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 2 de Application Server \(Solaris\)](#)
- [Actualización de la Versión 2 de Application Server \(Linux\)](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar Application Server, debe realizar las tareas siguientes:

- [Sólo para Solaris: Elimine manualmente los paquetes de Application Server integrados con el sistema operativo](#)
- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Application Server](#)
- [Copia de seguridad de los datos de Application Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Sólo para Solaris: Elimine manualmente los paquetes de Application Server integrados con el sistema operativo

La instalación de la Versión 2 de Application Server no ha eliminado la versión de Application Server integrada con el sistema operativo Solaris. Para actualizar correctamente Application Server de la Versión 2 a la Versión 5, tiene que llevar a cabo los siguientes pasos.

1. Desinstale la versión integrada eliminando manualmente los paquetes correspondientes de Application Server, que se encuentran en el directorio `/usr/appserver`:

```
pkgrm SUNWascmnse SUNWaslb SUNWasut ...
```

donde se puede obtener el conjunto completo de los paquetes utilizando el siguiente comando:

```
pkginfo -i|grep -i "application server"
```

Los resultados incluirán paquetes como, por ejemplo:

```
SUNWasacee, SUNWascmnse, SUNWasu, SUNWasuee, SUNWasac, SUNWascmn,
SUNWasdb, SUNWasdem, SUNWasdemdb, SUNWasr, SUNWasut, SUNWasman,
SUNWasjdoc
```

y también pueden incluir paquetes de traducción:

```
SUNWLocaleasacee, SUNWLocaleascmnse, SUNWLocaleasu, SUNWLocaleasuee
```

2. Si se ha utilizado la versión integrada, elimine la información de los dominios.

```
rm /usr/appserver/domains
```

Verifique la información sobre la versión actual

Para verificar la versión actual de Application Server, introduzca el siguiente comando:

```
AppServer7-base/bin/asadmin version --verbose
```

Consulte la [Tabla 11-5 en la página 229](#) para obtener información sobre la versión.

Actualización de las dependencias de Application Server

La actualización de las dependencias de Application Server requiere la actualización a la Versión 5 de todos los componentes de la Versión 2 de los que dependa Application Server, especialmente de Message Queue y de los componentes compartidos. Sin embargo, los componentes compartidos se actualizan automáticamente mediante el programa de instalación de Java ES como parte del procedimiento de actualización (consulte [“Procedimiento de actualización” en la página 239](#)).

Además, la actualización de Application Server requiere la instalación de HADB y de Java DB, de los que depende la Versión 5 de Application Server. Sin embargo, estos componentes compartidos son seleccionados e instalados automáticamente por el programa de instalación de Java ES como parte del procedimiento de actualización (consulte [“Procedimiento de actualización” en la página 239](#)).

Por lo general, al actualizar las dependencias de Application Server, tiene que seguir el orden que se indica a continuación (omitiendo cualquiera que ya se haya actualizado), antes de que actualice Application Server. Sin embargo, la actualización de los componentes compartidos, así como la instalación de HADB y de Java DB se realizan automáticamente mediante el programa de instalación de Java ES al actualizar Application Server.

1. **Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Application Server cuando realiza una actualización a la Versión 5 de Application Server.

NOTA La actualización de los componentes compartidos a la Versión 5 incluye la actualización de J2SE a JDK versión 1.5, que no es compatible con la Versión 2 de Application Server. Por lo tanto, antes de actualizar los componentes compartidos, deberá cerrar la Versión 2 de Application Server. Los componentes compartidos se actualizan a la Versión 5 siempre que se utilice el programa de instalación de Java ES para instalar o actualizar cualquier componente de producto de Java ES (por ejemplo Directory Server, Message Queue, HADB o Java DB, entre otros).

2. **Message Queue.** Consulte [“Actualización de Message Queue desde Java ES Versión 2” en la página 207](#). No se puede actualizar Message Queue desde la Versión 2 con el programa de instalación de Java ES.
3. **Almacén de sesión de alta disponibilidad (HADB).** Al actualizar Application Server, el programa de instalación de Java ES realiza una nueva instalación de HADB.
4. **Java DB.** Al actualizar Application Server, el programa de instalación de Java ES realiza una nueva instalación de Java DB.
5. **Software del contenedor web (dependencia leve de actualización).** Consulte [“Actualización de Web Server desde Java ES Versión 2” en la página 169](#).

Copia de seguridad de los datos de Application Server

Al actualizar Application Server de la Versión 2 a la Versión 5, no se sobrescriben los datos de configuración de la Versión 2. Sin embargo, como medida de seguridad, antes de realizar la actualización a la Versión 5 se debe realizar una copia de seguridad de todo el directorio domains:

AppServer7Config-base/domains

Obtenga las contraseñas y la información de configuración necesarias

Debe conocer la siguiente información sobre la versión instalada actualmente:

- Id. de usuario del administrador y contraseña de Application Server
- El directorio base de la Versión 2 de Application Server

Actualización de la Versión 2 de Application Server (Solaris)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Application Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Al actualizar el software de Application Server a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Deben cerrarse todos los componentes de J2EE que se estén ejecutando en una instancia de Application Server antes de actualizar dicha instancia. No obstante, este requisito no es imprescindible si se utiliza el equilibrado de carga para proporcionar alta disponibilidad o escalabilidad.
- Deben cerrarse todas las instancias de Application Server que se estén ejecutando en un único equipo (todas las que correspondan a la misma imagen de Application Server instalada) mientras se está actualizando la imagen instalada.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia a todas las instancias de Application Server que residen localmente en el equipo en el que vaya a realizarse la actualización.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Si los componentes compartidos de Java ES se han actualizado a la Versión 5 (en particular, si J2SE se ha actualizado a JDK 1.5) mientras que la Versión 2 de Application Server todavía se estaba ejecutando, edite el archivo `asenv.conf` para que señale directamente a JDK 1.4.

```
AS_JAVA=/usr/java
```

Application Server no se puede cerrar ([Paso 3](#), a continuación), si `asenv.conf` hace referencia a JDK 1.5.

3. Detenga todos los procesos de Application Server y demás procesos relacionados.

```
AppServer7-base/bin/asadmin stop-appserv domainName
```

4. Instale la Versión 5 de Application Server.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES en el equipo que aloje la Versión 2 de Application Server.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde `os_arch` coincide con la plataforma como, por ejemplo, `Solaris_sparc`. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden actualizarse directamente mediante el programa de instalación de Java ES, éstos aparecen con el estado “actualizable”.) Application Server *no* aparece como actualizable desde la Versión 2.

- b. Seleccione Application Server en la página de selección de componentes.

Decida si desea instalar, al menos, los tres primeros subcomponentes, incluido el Agente del nodo.

- c. Haga clic en Siguiente.

Si Message Queue todavía no se ha actualizado a la Versión 5, aparecerá una ventana de mensaje de error preguntándole si quiere actualizar Message Queue. En tal caso, haga clic en Aceptar y actualice Message Queue. El procedimiento se describe en [“Actualización de la Versión 2 de Message Queue” en la página 210](#).

- d. Especifique un directorio de instalación diferente del directorio en el que se instaló la Versión 2 de Application Server.
- e. Seleccione la opción Configurar más tarde.

NOTA	Si está en la versión de Application Server integrada con el sistema operativo Solaris 9 y nunca la ha utilizado (no se ha creado información de dominio), entonces puede seleccionar la opción Configurar ahora y omitir el Paso 5 y los sucesivos.
-------------	--

- f. Si fuera necesario, seleccione la opción para instalar paquetes traducidos.
 - g. Una vez completada la instalación, salga del programa de instalación de Java ES.
5. Lleve a cabo el siguiente procedimiento después de la instalación:

- a. Localice el archivo `readme postInstall` en el directorio de herramientas de Application Server de la distribución de la Versión 5 de Java ES:

Java ES Release 5 distribution/os_arch/Product/application_svr/Tools

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.

- b. Consulte el archivo `ReadMe` y ejecute la secuencia de comandos `postInstall`.

```
cd Java ES Release 5 distribution/os_arch/Product/application_svr/Tools
./postInstall AppServer8Install-base AppServer8Config-base
```

Las secuencias de comandos configuran y crean las secuencias de comandos del shell *AppServer8-base/bin/** y un archivo `config/asenv.conf` a partir de las plantillas instaladas durante la instalación. (Normalmente el programa de instalación de Java ES crea las secuencias de comandos del shell `bin/*`, pero si se ha seleccionado la opción Configurar más tarde, deben crearse como se describe a continuación).

NOTA Al actualizar Application Server a la Versión 5, los puertos no administrativos 8080 (predeterminado) y 8181 (seguro) están ubicados en el Domain Administration Server (DAS). Es posible que estas asignaciones de puertos produzcan conflictos con los puertos ubicados en las instancias de la Versión 2 de Application Server. Si se diera el caso, debería cambiar los puertos de DAS para evitar cualquier conflicto. Para obtener más instrucciones, consulte la sección sobre cómo modificar atributos http-listener en la *Sun Java System Application Server Enterprise 8.2 Edition Administration Guide*, <http://docs.sun.com/doc/819-4733>.

- c. Si es necesario, modifique la configuración del entorno en el archivo *AppServer8-base/config/asenv.conf* .

Puede editar este archivo manualmente.

NOTA Para configurar Application Server para el equilibrado de carga, consulte la sección configuración de los servidores Web para el equilibrado de carga HTTP, “Configuring Web Servers for HTTP Load Balancing”, en el capítulo “Application Server High Availability Features” de la *Sun Java System Application Server Enterprise 8.2 Edition High Availability Administration Guide*, <http://docs.sun.com/doc/819-4740>.

6. Ejecute la utilidad asupgrade.

La utilidad asupgrade crea un agente de nodo de la Versión 5 bajo el que se migran las instancias de Application Server de la Versión 2.

La utilidad se encuentra en el directorio de Application Server, por ejemplo:

- Modo de asistente de actualización: *AppServer8-base/bin/asupgrade*
- Modo de consola de actualización: *AppServer8-base/bin/asupgrade -c*

El asistente o la consola de actualización le guiarán por el procedimiento de actualización.

- a. Identifique el directorio de origen y el de destino para la migración de la información de los dominios:

- Versión 2: *AppServer7-base*
 - Versión 5: *AppServerConfig8-base/domains*
- b. Proporcione el usuario administrador, la contraseña de administrador y la contraseña maestra de la Versión 2 de Application Server.

Si se le pide una contraseña maestra, especifique `changeit` y, si está utilizando una clave de agente que tenga una contraseña maestra diferente de `changeit`, cámbiela por `changeit`.

```
jdk-home/bin/keytool -storepasswd -new changeit -keystore keystore
-storepass oldpasswd
```

Para más información sobre la utilidad `asupgrade` de Application Server, consulte la sección de comandos de usuario del *Sun Java System Application Server Enterprise Edition 8.2 Reference Manual*, <http://docs.sun.com/doc/819-4736> y la *Guía de migración y actualización de Sun Java System Application Server Enterprise Edition 8.2*, <http://docs.sun.com/doc/819-4737/6n6sao3ju?a=view>.

7. Si ha redirigido el archivo `asenv.conf` en el [Paso 2 en la página 240](#), restáurelo para que señale a JDK 1.5.

```
AS_JAVA=/usr/jdk/entsys-j2se
```

Application Server no se puede iniciar ([Paso 8](#) y [Paso 9](#), a continuación) si `asenv.conf` hace referencia a JDK 1.4.

8. Inicie Domain Administration Server (DAS).

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

9. Reinicie las instancias actualizadas de Application Server.

Para ello, inicie el agente del nodo en el que se han migrado las instancias de Application Server actualizadas:

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
nodeagentName
```

donde `nodeagentName` presenta el formato `hostName_domainName`, pero es sólo de forma predeterminada `hostName`.

Actualización de la Versión 2 de Application Server (Linux)

La actualización de Application Server de la Versión 2 a la Versión 5 en la plataforma Linux se complica por el hecho de que Java ES Versión 2 sólo se admite en RHEL 2.1, pero Java ES Versión 5 no se admite en RHEL 2.1. Por lo tanto, es necesaria una actualización doble: deben actualizarse tanto el sistema operativo como Application Server. Consulte [“Actualizaciones dobles: El software de Java ES y el sistema operativo” en la página 46](#).

El procedimiento básico que seguir consiste en actualizar primero el sistema operativo Linux, después todas las dependencias de Application Server y, por último, Application Server, siguiendo el mismo procedimiento descrito en [“Actualización de la Versión 2 de Application Server \(Solaris\)” en la página 239](#).

Verificación de la actualización

Inicie la consola de administración y compruebe que se inician estos servidores. Si no se ejecuta alguno de estos servidores, consulte el siguiente archivo de registro para conocer los fallos que hayan podido ser provocados por conflictos de puertos:

AppServer8Config-base/nodeagents/nodeagentName/instanceName/logs/server.log

Si se produce algún error debido a conflictos de puertos, utilice la consola de administración para modificar los números de puertos de forma y eliminar de esta forma los conflictos. A continuación, detenga y reinicie el agente del nodo.

Puede verificar la actualización de Application Server a la Versión 5 introduciendo el siguiente comando:

AppServer8-base/bin/asadmin version --verbose

Consulte la [Tabla 11-5 en la página 229](#) para obtener los valores de salida.

Tareas posteriores a la actualización

Una vez finalizada la actualización, deberá llevar a cabo dos tareas, además de las descritas en [“Procedimiento de actualización” en la página 239](#):

- [Corrija la referencia a JSS](#)
- [Migre los componentes de la Versión 2 de J2EE](#)

Corrija la referencia a JSS

Para que Application Server haga referencia a la versión correcta del componente compartido JSS, debe sustituir `jss3.jar` por `jss4.jar` en el archivo de Application Server `domain.xml` ubicado en:

AppServer8Config-base/domains/domainName/config/domain.xml

Migre los componentes de la Versión 2 de J2EE

Tiene que migrar las aplicaciones y los componentes de la Versión 2 de J2EE para que se ejecuten en un entorno de Application Server de la Versión 5 y se implementen en las instancias adecuadas de Application Server. Para más información sobre cómo migrar las aplicaciones y los componentes de J2EE, consulte el Capítulo 4 de la *Application Server Enterprise Edition 8.2 Upgrade and Migration Guide*, <http://docs.sun.com/doc/819-4737>.

Anulación de la actualización

Para deshacer la actualización de Application Server a la Versión 5, basta con restablecer la Versión 2 de Application Server, que no se había eliminado durante la actualización.

Actualización de Application Server integrado en Solaris en un entorno de zonas múltiples de Solaris 10

Application Server (así como Message Queue, del que depende Application Server), está integrado en el sistema operativo Solaris 10. A no ser que se elimine de la zona global, Application Server integrado se propaga a zonas no globales cuando se crean dichas zonas. La existencia de Application Server integrado en todas las zonas afecta a la posterior actualización a la Versión 5 de Application Server:

- Al actualizar Application Server en la zona global, se elimina la versión integrada de la zona global y se elimina también automáticamente de todas las zonas no globales.
- La actualización de Application Server a la Versión 5 en la zona global no implica la actualización de Application Server en las zonas no globales, puesto que los paquetes de Application Server de la Versión 5 no se propagan.

El siguiente ejemplo ilustra algunos de los aspectos delicados de una actualización de Application Server en un entorno de zonas múltiples de Solaris 10. (Para una discusión más exhaustiva relacionada con Java ES y las zonas de Solaris 10, consulte [“Actualización a Java ES 5 y zonas de Solaris 10” en la página 62.](#))

En este ejemplo, el objetivo es actualizar a la Versión 5 Application Server (versión 8.0.0_01) integrado en Solaris en una zona root dispersa de Solaris 10.

No puede actualizar simplemente Application Server en una zona root dispersa porque Application Server integrado en Solaris está instalado en un directorio de sólo lectura montado desde la zona global. Por lo tanto, actualice Application Server a la Versión 5 en la zona root dispersa. Para ello debe eliminar primero la versión integrada de la zona global.

Además, Message Queue está instalado en la zona global y representa una novedad en la práctica, ya que sólo los componentes compartidos (no los componentes de los productos) se instalarán en la zona global. Esto ocurre porque Message Queue no se puede instalar o actualizar en una zona root dispersa debido a los directorios de sólo lectura.

El procedimiento para actualizar a la Versión 5 Application Server (versión 8.0.0_01) integrado en Solaris en una zona root dispersa de Solaris 10 es el siguiente:

1. Verifique el estado inicial de su sistema.

En este ejemplo se supone que la zona root dispersa de la versión de Solaris 10 ha sido configurada, instalada e iniciada por el administrador global.

La zona root dispersa incluye todos los componentes de Java ES que ya han sido instalados en la zona global, concretamente las versiones de Message Queue y de Application Server integrados en Solaris 10.

Además, en el ejemplo se supone que el usuario ha utilizado previamente Application Server integrado en la zona root dispersa y que ha creado información administrativa del dominio que es preciso conservar.

2. Actualice la versión integrada de Application Server en la zona global.

Esta operación elimina los paquetes integrados de Application Server y los sustituye por paquetes de la Versión 5. La eliminación de los paquetes integrados se propaga a la zona root dispersa; en concreto, los paquetes de Application Server se desinstalan en la zona root dispersa, pero los paquetes de la Versión 5 no se propagan a las zonas no globales.

- a.** Ejecute el programa de instalación de Java ES en la zona global.
- b.** Seleccione Application Server en la página de selección de componentes.
Message Queue, HADB y Java DB se seleccionarán automáticamente y Application Server y Message Queue se marcarán como actualizables.
- c.** Complete la instalación.

Mientras que la Versión 5 de Message Queue se propaga a la zona root dispersa, ni Application Server, HADB, ni Java DB se propagarán. Además, todos los componentes compartidos se sincronizarán en la Versión 5 y se propagarán a la zona root dispersa.

3. Instale Application Server en la zona root dispersa.

- a.** Ejecute el programa de instalación de Java ES en la zona root dispersa.
- b.** Seleccione Application Server en la página de selección de componentes.
Si Message Queue se selecciona automáticamente, elimine dicha selección y seleccione HADB y Java DB en caso de que no se hayan seleccionado automáticamente.

c. Complete la instalación de Application Server.

Seleccione la opción Configurar más tarde, para que la información de dominio no se sobrescriba en el proceso de instalación.

En el caso de que no se haya creado ningún dominio, seleccione Configurar ahora.

Service Registry

En este capítulo, se describe cómo actualizar Service Registry a Java ES 5 (Versión 5): Service Registry 3.1.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de las actualizaciones de Service Registry” en la página 251
- “Actualización de Service Registry desde Java ES Versión 4” en la página 254

NOTA	Las ubicaciones de los archivos en este capítulo se especifican en relación con las rutas de directorio a las que se denominan <i>ServiceRegistryR4-base</i> y <i>RegistryDomainR4-base</i> (Service Registry de Java ES Versión 4), y <i>ServiceRegistryR5-base</i> y <i>RegistryDomainR5-base</i> (Service Registry de Java ES Versión 5). Debe haberse especificado, al menos, una parte de estas rutas como directorios de instalación durante la instalación de Service Registry. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado. Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.
-------------	---

Tabla 12-1 Service Registry Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>ServiceRegistryR4-base</i>	/opt/SUNWsoar	/opt/sun/SUNWsoar
<i>RegistryDomainR4-base</i>	/var/opt/SUNWsoar	/var/opt/sun/SUNWsoar

Tabla 12-1 Service Registry Rutas de directorio (*continúa*)

Variable de nombre de ruta	SO Solaris	SO Linux
<i>ServiceRegistryR5-base</i>	/opt/SUNWsrcv-registry	/opt/sun/srcv-registry
<i>RegistryDomainR5-base</i>	/var/opt/SUNWsrcv-registry	/var/opt/sun/srcv-registry

Visión general de las actualizaciones de Service Registry

En esta sección se describen los siguientes aspectos generales de Service Registry que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Java ES Versión 5](#)
- [Guía de actualización deJava ES Versión 5](#)
- [Datos de Service Registry](#)
- [Estrategia de actualización para Service Registry](#)

Acerca de Java ES Versión 5

Service Registry de Java ES Versión 5 representa una versión inferior en relación con la Versión 4 de Service Registry. Incluye algunas funciones mejoradas, interfaces actualizadas y soluciones de errores exclusivas.

Guía de actualización deJava ES Versión 5

La [Tabla 12-2](#) muestra las rutas de actualización compatibles de Service Registry para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 12-2 Rutas de actualización a Java ES 5 (Versión 5): Service Registry 3.1

Versión de Java ES	Service Registry Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Service Registry 3.0 2005Q4	Actualización directa: Sustituya la Versión 4 con una instalación nueva y transfiera los datos de registro a la Versión 5.	Ninguna

Datos de Service Registry

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Service Registry.

Tabla 12-3 Uso de datos de Service Registry

Tipo de datos	Ubicación	Uso
Parámetros de instalación	<i>ServiceRegistryR4-base/install/install.properties</i>	Configuración de Service Registry
Certificados de confianza	<i>ServiceRegistryR4-base/install/cacerts</i>	Certificados en los que confía Service Registry que no forman parte de la instalación de Application Server
Datos de configuración	<i>RegistryDomainR4-base/domains/registry/applications/j2ee-modules/soar/WEB-INF/classes/*.properties</i>	Configuración de la instancia de Service Registry
Datos de registro o del depósito	<i>RegistryDomainR4-base/3.0/data</i>	Bases de datos y certificados de usuario
Configuración de interfaz web	<i>RegistryDomainR4-base/3.0/jaxr-ebxml</i>	Configuración de interfaz web

Estrategia de actualización para Service Registry

La estrategia utilizada para la actualización de Service Registry depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Service Registry presentando una serie de problemas que pueden influir en el plan de actualización de Service Registry.

Problemas de compatibilidad

La Versión 5 de Service Registry es compatible con la Versión 4 de Service Registry.

Dependencias

Las dependencias de Service Registry con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Service Registry. Por ejemplo, los cambios en las interfaces o las funciones de Service Registry pueden requerir las versiones actualizadas de los componentes de los que depende Service Registry. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Service Registry presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Service Registry presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Application Server.** Service Registry presenta una relación de dependencia obligatoria con Application Server para proporcionar un contenedor a la aplicación de Service Registry y, en Java ES Versión 5, para administrar las conexiones de la base de datos de registro/depósito en red.
- **Java DB.** Service Registry presenta una relación de dependencia obligatoria con Java DB como base de datos predeterminada para almacenar los servicios y los metadatos que los describen.

Actualización de Service Registry desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Service Registry desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Service Registry](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Service Registry de Java ES de la Versión 4 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** La actualización se consigue mediante una instalación nueva de la Versión 5 de Service Registry, la migración de los datos y la configuración de la Versión 4 a la Versión 5 y, por último, la eliminación de la Versión 4 para conservar el espacio en disco.
- **Dependencias de actualización.** Service Registry presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realice una actualización de Service Registry.

Service Registry presenta fuertes relaciones de dependencia con Application Server y Java DB.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Service Registry es totalmente compatible con la Versión 4.
- **Anulación de la actualización.** Para deshacer la actualización de la Versión 5 se debe restablecer la Versión 4 después de haber restaurado la base de datos y los datos de configuración guardados.
- **Problemas de plataforma.** El enfoque general de actualización de Service Registry es idéntico tanto para el sistema operativo Solaris como para Linux.

Actualización de la Versión 4 de Service Registry

En esta sección se describe cómo realizar una actualización de Service Registry desde Java ES Versión 4 a la Versión 5 de Java ES en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Service Registry](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar Service Registry, debe realizar las tareas siguientes:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Service Registry](#)
- [Copia de seguridad de los datos de Service Registry](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Puede verificar la versión actual de Service Registry observando las características de la interfaz de usuario de la consola web:

```
http://localhost:6060/soar
```

También puede comprobar los nombres de los paquetes de Service Registry. Por ejemplo:

En Solaris:

```
pkginfo -l|grep svc
```

En Linux:

```
rpm -qa|grep svc
```

Las características diferenciadoras y los nombres de los paquetes se muestran en la siguiente tabla:

Tabla 12-4 Resultados de la verificación de la versión de Service Registry

Versión de Java ES	Número de versión de Service Registry	Características diferenciadoras
Versión 4	3.0	Consola web: sección de herramientas en el panel izquierdo Los nombres de los paquetes incluyen la cadena: soar
Componente de producto de la	3.1	Consola web: tres tabuladores en el panel izquierdo Los nombres de los paquetes incluyen la cadena: svc-registry

Actualización de las dependencias de Service Registry

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Service Registry presenta fuertes relaciones de dependencia con varios componentes compartidos de Application Server y de Java DB.

Al actualizar las dependencias de Service Registry, debe seguir el orden que le mostramos a continuación (omitiendo cualquiera que ya se haya actualizado), antes de actualizar Service Registry. Normalmente, el programa de instalación de Java ES realiza automáticamente la actualización de los componentes compartidos.

- 1. Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Service Registry cuando realiza una actualización a la Versión 5 de Service Registry.
- 2. Java DB.** Las instrucciones para actualizar Java DB a la Versión 5 están disponibles en el [Capítulo 8, “Java DB” en la página 171](#).
- 3. Application Server.** Las instrucciones para actualizar Application Server a la Versión 5 están disponibles en el [Capítulo 11, “Application Server” en la página 219](#).

Modifique el número de puerto HTTP

Edite el archivo *ServiceRegistryR4-base/install/install.properties* para cambiar el puerto HTTP de 6060 a 6480 (6060 es un puerto reservado). Para obtener más información sobre cómo establecer esta propiedad, consulte la *Service Registry 3.1 Administration Guide*, <http://docs.sun.com/doc/819-4640>.

Copia de seguridad de los datos de Service Registry

Al actualizar Service Registry de la Versión 4 a la Versión 5 no se modifican los datos de configuración ni las bases de datos de registro/depósito, por lo que no es necesario que realice una copia de seguridad de los datos actuales.

Obtenga las contraseñas y la información de configuración necesarias

Tendrá que conocer los Id. de usuario, las contraseñas, el nombre de dominio y el número de puerto para la Versión 4 de Service Registry.

Actualización de la Versión 4 de Service Registry

En esta sección se describe el procedimiento de actualización en las plataformas Solaris y Linux.

Procedimiento de actualización (Solaris)

El procedimiento que se describe a continuación hace referencia a las instancias de Service Registry que residen localmente en el equipo en el que se vaya a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

```
su -
```

2. Asegúrese de que la herramienta de creación basada en Jakarta ANT Java/XML (componente compartido ANT) hace referencia a la versión correcta de J2SE.

(El comando ant se utiliza en los pasos que aparecen a continuación.)

```
PATH=/usr/jdk/entsys-j2se/bin:$PATH
```

```
export PATH
```

3. Detenga el dominio de la Versión 4 de Service Registry (Application Server).

```
cd ServiceRegistryR4-base/install
```

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.stop
```

El dominio está asociado con una instancia de Service Registry.

4. Realice una nueva instalación de la Versión 5 de Service Registry.

Lleve a cabo estos pasos:

- a.** Inicie el programa de instalación de Java ES en el equipo que aloje la Versión 4 de Service Registry.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción *installer -nodisplay* para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b.** Seleccione Service Registry en la página de selección de componentes.
- c.** Especifique una ruta de directorio de instalación diferente de la ruta de la Versión 4.

Por defecto, la ruta de instalación de la Versión 5 (*ServiceRegistryR5-base*) es diferente de la ruta de la Versión 4 (*ServiceRegistryR4-base*).

- d.** Seleccione la opción Configurar más tarde.

No se admite Configurar ahora.

- e.** Si fuera necesario, seleccione la opción para instalar paquetes traducidos.
- f.** Una vez completada la instalación, salga del programa de instalación de Java ES.

5. Actualice y configure la instancia de Service Registry de la Versión 5.

```
cd ServiceRegistryR5-base/install
/usr/sfw/bin/ant -f build-install.xml
-Dinstall.properties=ServiceRegistryR4-base/install/install.properties
upgrade
```

Como alternativa a señalar a la Versión 4 del archivo *install.properties*, puede modificar el archivo predeterminado *install.properties* de la Versión 5 para modificar cualquier valor de propiedad de la Versión 4. Para más información sobre cómo establecer estas propiedades, consulte la *Service Registry 3.1 Administration Guide*, <http://docs.sun.com/doc/819-4640>.

Si está utilizando valores de propiedad personalizados, pero no los está poniendo en `install.properties`, entonces tendrá que especificar dichos valores de propiedad en la línea de comandos Ant (todo en la misma línea), como se indica a continuación:

```
/usr/sfw/bin/ant -f build-install.xml
-Dregistry.install.RegistryServerKeystorePassword=password1
-Dregistry.install.AdministratorPassword=password2
-Dregistry.install.ApplicationServerKeystorePassword=password3
upgrade
```

Sin embargo, es recomendable que incluya dichos valores de propiedad personalizados en el archivo `install.properties` con acceso restringido para evitar el uso de la configuración de la línea de comandos por personas no autorizadas que puedan verla. Consulte la *Service Registry Administration Guide* para obtener más información.

La utilidad de actualización crea un dominio nuevo de Application Server, inicia el dominio e implementa las instancias de Service Registry en él. Cada instancia de Service Registry está asociada con su propio dominio de Application Server.

6. Si se han modificado los archivos de propiedad del servidor de la Versión 4 de Service Registry, puede hacer los cambios correspondientes en la configuración de la Versión 5 de Service Registry, siguiendo las instrucciones descritas a continuación:

- a. Detenga el dominio de la Versión 5 de Service Registry (Application Server).

(El dominio se inició automáticamente mediante el comando `upgrade` del [Paso 5](#).)

```
cd ServiceRegistryR5-base/install
/usr/sfw/bin/ant -f build-install.xml appserver.domain.stop
```

- b. Transfiera la configuración de la instancia de Service Registry de la Versión 4 a la Versión 5.

Añada cualquier modificación que haya realizado en la configuración de la instancia de la Versión 4 de Service Registry:

```
RegistryDomainR4-base/domains/registry/applications/j2ee-modules/  
soar/WEB-INF/classes/*.properties
```

a la configuración correspondiente de la Versión 5:

```
RegistryDomainR5-base/domains/registry/applications/j2ee-modules/  
soar/WEB-INF/classes/*.properties
```

7. Inicie el dominio de la Versión 5 de Service Registry (Application Server).

```
cd ServiceRegistryR5-base/install  
/usr/sfw/bin/ant -f build-install.xml appserver.domain.start
```

Procedimiento de actualización (Linux)

La actualización de Service Registry en la plataforma Linux es igual que en Solaris (consulte [“Procedimiento de actualización \(Solaris\)” en la página 257](#)) excepto que la ubicación del comando ant en la plataforma Linux, comando que se utiliza en varios pasos del procedimiento de actualización, es diferente de su ubicación en las plataformas Solaris:

```
/opt/sun/share/bin/ant
```

Verificación de la actualización

Puede verificar si la actualización de Service Registry se ha realizado correctamente observando las características de la interfaz de usuario de la consola web:

```
http://localhost:6480/soar
```

También puede comprobar los nombres de los paquetes de Service Registry. Por ejemplo:

En Solaris:

```
pkginfo -l|grep soar
```

En Linux:

```
rpm -qa|grep soar
```

Las características diferenciadoras y los nombres de los paquetes se muestran en la [Tabla 12-4 en la página 256](#).

Tareas posteriores a la actualización

Los pasos que aparecen a continuación, y que describen cómo eliminar la Versión 4 de Service Registry, no deben realizarse hasta que esté seguro de que no quiere deshacer la actualización a la Versión 4.

1. Elimine el dominio de la Versión 4 de Service Registry (Application Server):

```
cd ServiceRegistryR4-base/install
```

En Solaris:

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.delete
```

En Linux:

```
/opt/sun/bin/ant -f build-install.xml appserver.domain.delete
```

2. Elimine el directorio que contiene los archivos de dominio de la Versión 4 de Service Registry.

```
rm -rf RegistryDomainR4-base
```

3. Elimine el directorio que contiene los archivos de instalación de la Versión 4 de Service Registry.

```
rm -rf ServiceRegistryR4-base
```

Anulación de la actualización

Para deshacer la actualización a la Versión 5 se debe eliminar la versión anterior, que se mantiene intacta al actualizar a la Versión 5.

1. Detenga y borre el dominio de la Versión 5 de Service Registry (Application Server):

```
cd ServiceRegistryR4-base/install
```

En Solaris:

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.delete
```

En Linux:

```
/opt/sun/bin/ant -f build-install.xml appserver.domain.delete
```

2. Ejecute el programa de desinstalación de Java ES Versión 5 para desinstalar la Versión 5 de Service Registry.

3. Inicie el dominio de la Versión 4 de Service Registry.

```
cd ServiceRegistryR4-base/install
```

En Solaris:

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.start
```

En Linux:

```
/opt/sun/bin/ant -f build-install.xml appserver.domain.start
```

4. Acceda a la Versión 4 de la consola web de Service Registry.

```
http://localhost:6480/soar
```

5. Confirme que la consola muestra las características de la Versión 4 como se indica en [“Resultados de la verificación de la versión de Service Registry” en la página 256](#).

Actualización de varias instancias

En algunas arquitecturas de implementación, Service Registry se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que las instancias de Service Registry se ejecuten en varios equipos con un equilibrador que distribuya la carga.

En este tipo de arquitecturas, los registros son fundamentalmente de sólo lectura y responden a una carga de consulta pesada cuando se accede a una base de datos común.

Debe realizar la actualización de Service Registry en todos los equipos tal y como se describe en [“Actualización de la Versión 4 de Service Registry” en la página 255](#).

Web Proxy Server

En este capítulo se describe cómo actualizar Web Proxy Server a Java ES 5 (Versión 5): Sun Java System Web Proxy Server 4.0.4.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Web Proxy Server” en la página 264
- “Actualización de Web Proxy Server desde Java ES Versión 4” en la página 267
- “Actualización de Web Proxy Server desde la Versión 3.6” en la página 274

NOTA Las ubicaciones de los archivos de este capítulo se especifican en relación con la ruta de directorio a la que se denomina *WebProxyServer-base*. Debe haberse especificado, al menos, parte de esta ruta como directorio de instalación durante la instalación inicial de Web Proxy Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado.

El valor predeterminado de *WebProxyServer-base* depende de la plataforma de sistema operativo que se utilice, como se describe en la siguiente tabla:

Tabla 13-1 Web Proxy Server Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>WebProxyServer-base</i>	/opt/SUNWproxy	/opt/sun/webproxyserver

Visión general de la actualización de Web Proxy Server

En esta sección se describen los siguientes aspectos generales de Web Proxy Server que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Web Proxy Server de Java ES Versión 5](#)
- [Guía de actualización de Web Proxy Server](#)
- [Datos de Web Proxy Server](#)
- [Estrategia de actualización para Web Proxy Server](#)

Acerca de Web Proxy Server de Java ES Versión 5

Web Proxy Server de Java ES Versión 5 representa una versión inferior en cuanto a la solución de problemas con respecto a la Versión 4.

Sin embargo, la Versión 5 de Web Proxy Server presenta un mejor rendimiento, una arquitectura más escalable, mejor compatibilidad con estándares y una nueva interfaz de administración en comparación con Sun One Web Proxy Server 3.6 antes de su inclusión en Java Enterprise System.

Guía de actualización de Web Proxy Server

La [Tabla 13-2](#) muestra la ruta de actualización de Web Proxy Server a Java ES Versión 5. Web Proxy Server no se incluía en las versiones anteriores de Java ES. Esta tabla sólo hace referencia al sistema operativo Solaris, ya que Web Proxy Server no era compatible anteriormente con el sistema operativo Linux.

Tabla 13-2 Rutas de actualización a Java ES 5 (Versión 5): Web Proxy Server 4.0.4

Versión de Java ES	Web Proxy Server Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Web Proxy Server 4.0.1 2005Q4	Actualización directa: Se realiza mediante revisiones	Ninguna

Tabla 13-2 Rutas de actualización a Java ES 5 (Versión 5): Web Proxy Server 4.0.4

Versión de Java ES	Rutas de actualización a Java ES 5 (Versión 5): Web Proxy Server 4.0.4		
	Web Proxy Server Versión	Enfoque general	Reconfiguración necesaria
Versiones anteriores de Java ES (sólo para el SO Solaris)	Sun ONE Web Proxy Server 3.6 (A continuación, pasará a denominarse Versión 3.6)	Actualización directa: Se realiza mediante el programa de instalación de Java ES que permite realizar la instalación en una nueva ubicación y migrar a continuación los datos de configuración mediante las herramientas de administración.	La información de configuración debe migrarse a la nueva ubicación.

Datos de Web Proxy Server

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Web Proxy Server.

Tabla 13-3 Uso de datos de Web Proxy Server

Tipo de datos	Ubicación	Uso
Datos de configuración	<i>WebProxyServer-base/proxy-serverid/config</i> directory Contiene archivos del tipo: <i>server.xml</i> , <i>magnus.conf</i> , <i>obj.conf</i> , etc.	Almacena información de configuración del servidor, la memoria caché, los filtros, la función de enrutamiento y otros aspectos funcionales de Web Proxy Server

Estrategia de actualización para Web Proxy Server

La estrategia utilizada para la actualización de Web Proxy Server depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Web Proxy Server presentando una serie de problemas que pueden influir en el plan de actualización de Web Proxy Server.

Problemas de compatibilidad

La Versión 5 de Web Proxy Server no incluye ninguna interfaz pública nueva y es compatible con la Versión 4 de Web Proxy Server. La Versión 5 de Web Proxy Server es compatible con la Versión 3.6, aunque se deben volver a compilar los complementos desarrollados mediante la interfaz NSAPI admitida por la Versión 3.6 en la interfaz NSAPI compatible con la Versión 5.

Web Proxy Server Dependencias

Web Proxy Server presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Web Proxy Server presenta relaciones de dependencia con componentes compartidos específicos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Directory Server.** Web Proxy Server presenta una relación de dependencia opcional con Directory Server para proporcionar autenticación basada en LDAP.
- **Web Server.** Web Proxy Server presenta una relación de codependencia con Web Server para proporcionar mejoras en el rendimiento y la seguridad de las solicitudes HTTP.

Actualización de Web Proxy Server desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Web Proxy Server desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Web Proxy Server](#)

Introducción

Al actualizar Web Proxy Server a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** La actualización se lleva a cabo mediante revisiones. No es necesaria ninguna reconfiguración adicional.
- **Dependencias de actualización.** Web Proxy Server tiene relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Sin embargo, Web Proxy Server tiene dependencias fuertes de actualización sólo con los componentes compartidos NSS y NSPR.
- **Compatibilidad con versiones anteriores.** La Versión 5 de Web Proxy Server es compatible con la Versión 4.
- **Anulación de la actualización.** La anulación de la actualización de la Versión 5 de Web Proxy Server se consigue eliminando las revisiones de actualización.
- **Problemas de plataforma.** El enfoque de actualización general de Web Proxy Server es idéntico tanto en el sistema operativo Solaris como en Linux. No obstante, las tecnologías de aplicación de revisiones son distintas. Por lo tanto, el proceso de actualización incluye procedimientos específicos para cada plataforma.

Actualización de la Versión 4 de Web Proxy Server

En esta sección se describe cómo llevar a cabo una actualización de Web Proxy Server a Java ES Versión 5. La sección cubre los siguientes puntos:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Web Proxy Server \(Solaris\)](#)
- [Actualización de la Versión 4 de Web Proxy Server \(Linux\)](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Deshacer la actualización \(Solaris\)](#)

Tareas previas a la actualización

Antes de actualizar Web Proxy Server, debe realizar las tareas siguientes:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Web Proxy Server](#)
- [Copia de seguridad de los datos de Web Proxy Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Web Proxy Server, introduzca el siguiente comando:

```
WebProxyServer-base/proxy-admserv/start -version
```

Tabla 13-4 Web Proxy Server Resultados de la verificación de la versión

Versión de Java ES	Número de versión de Web Proxy Server
Versión 3.6, no asociada a ninguna versión de Java ES	3.6
Versión 4	4.0.1
Componente de producto de la	4.0.4

Actualización de las dependencias de Web Proxy Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Sin embargo, la actualización de Web Proxy Server a la Versión 5 sólo requiere que se actualicen los componentes compartidos NSS y NSPR. Si todavía no se han actualizado estos componentes compartidos, debe sincronizar todos los componentes compartidos en la Versión 5 mediante la opción de Sincronización de componentes compartidos. Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#) en la página 69.

Copia de seguridad de los datos de Web Proxy Server

Al actualizar Web Proxy Server a la Versión 5, no se modifican los datos de configuración de la Versión 4, por lo que no es necesario que realice una copia de seguridad de los datos actuales.

Obtenga las contraseñas y la información de configuración necesarias

No es necesaria ninguna información especial sobre la versión instalada actualmente. Sin embargo, deberá iniciar sesión como superusuario para realizar la actualización.

Actualización de la Versión 4 de Web Proxy Server (Solaris)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Web Proxy Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización (Solaris)

Al actualizar el software de Web Proxy Server a Java ES Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Todas las instancias de Web Proxy Server correspondientes a la misma imagen instalada de Web Proxy Server se actualizan al mismo tiempo. Todas estas instancias deben cerrarse al aplicar las revisiones en la imagen instalada.
- Las revisiones de actualización de la Versión 5 de Web Proxy Server para el SO Solaris se muestran en la siguiente tabla:

Tabla 13-5 Revisiones¹ de actualización de Web Proxy Server en Solaris

Descripción	Id. de revisión: SPARC Solaris 9 y 10	Id. de revisión: x86 Solaris 9 y 10
Núcleo de Web Proxy Server	120981-06	120982-06

Tabla 13-5 Revisiones¹ de actualización de Web Proxy Server en Solaris (*continúa*)

Descripción	Id. de revisión: SPARC Solaris 9 y 10	Id. de revisión: x86 Solaris 9 y 10
Traducción de Web Proxy Server	122963-01	122964-01

1. Los números de revisiones suponen la revisión mínima necesaria para actualizar a Java ES Versión 5. Si aparecen nuevas revisiones, utilícelas en lugar de las que aparecen en la tabla.

Procedimiento de actualización (Solaris)

El procedimiento que se describe a continuación hace referencia a Web Proxy Server en el equipo en el que se vaya a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

su -
2. Detenga todas las instancias de Web Proxy Server y del servidor de administración que se estén ejecutando.

WebProxyServer-base/proxy-instanceName/stop
WebProxyServer-base/proxy-admserv/stop
3. Si todavía no ha llevado a cabo esta tarea, sincronice todos los componentes compartidos en la Versión 5.

Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#) en la página 69.
4. Obtenga los números de revisión necesarios en la [Tabla 13-5](#).

Las revisiones pueden descargarse en /tmp desde:
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
5. Aplique el núcleo adecuado de Web Proxy Server y, si fuera necesario, las revisiones de localización que aparecen en la [Tabla 13-5](#), en ese orden.

patchadd /tmp/patch_ID
6. Confirme que las actualizaciones de las revisiones se han realizado con éxito:

showrev -p | grep proxy

Como resultado, deberían devolverse las versiones de Id. de revisión aplicadas en el [Paso 5](#).

7. Reinicie las instancias de Web Proxy Server que se detuvieron en el [Paso 2](#).
WebProxyServer-base/proxy-instanceName/start

Actualización de la Versión 4 de Web Proxy Server (Linux)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Web Proxy Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización (Linux)

Al actualizar el software de Web Proxy Server a Java ES Versión 5 en la plataforma Linux, es preciso tener en cuenta las mismas consideraciones que en la plataforma Solaris (consulte [“Consideraciones sobre la actualización” en la página 276](#)), excepto que las revisiones de actualización de la Versión 5 para Linux sean diferentes de las de Solaris.

Las revisiones de actualización de la Versión 5 de Web Proxy Server para el SO Linux se muestran en la siguiente tabla:

Tabla 13-6 Revisiones¹ de actualización de Web Proxy Server en Linux

Descripción	Id. de parche y nombres de RPM
Núcleo de Web Proxy Server	120983-06 sun-proxyserver-4.0-6.5.i386.rpm
Traducción de Web Proxy Server	122965-01 sun-proxyserver-Locale-4.0.4.i386.rpm

1. Los números de revisiones suponen la revisión mínima necesaria para actualizar a Java ES Versión 5. Si aparecen nuevas revisiones, utilícelas en lugar de las que aparecen en la tabla.

Procedimiento de actualización (Linux)

El procedimiento que se describe a continuación hace referencia a Web Proxy Server en el equipo en el que se vaya a realizar la actualización.

PRECAUCIÓN En Linux, la actualización de Java ES Versión 4 a Java ES Versión 5 no se puede deshacer.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Detenga todas las instancias de Web Proxy Server que se estén ejecutando y el servidor de administración.

```
WebProxyServer-base/proxy-instanceName/stop
WebProxyServer-base/proxy-admserv/stop
```

3. Si todavía no ha llevado a cabo esta tarea, sincronice todos los componentes compartidos en la Versión 5.

Consulte el “[Actualización de las dependencias de Web Proxy Server](#)” en la [página 269](#).

4. Obtenga las revisiones necesarias utilizando los números de revisión y los nombres de RPM de la [Tabla 13-6](#). Use esta información para obtener los números de versión para el RPM.

Las revisiones pueden descargarse en /tmp desde:
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

5. Aplique el núcleo y, si fuera necesario, los RPM de traducción en Web Proxy Server según lo que se muestra en la [Tabla 13-6](#), en ese orden.

```
rpm -Fvh sun-proxyserver-version.i386.rpm
```

6. Confirme que las actualizaciones de las revisiones se han realizado con éxito:

```
rpm -qa | grep sun-proxyserver
```

Se deberían mostrar los números de las nuevas versiones de los RPM.

7. Reinicie las instancias de Web Proxy Server que se detuvieron en el [Paso 2](#).

```
WebProxyServer-base/proxy-instanceName/start
```

Verificación de la actualización

Puede verificar la actualización de Web Proxy Server a la Versión 5 iniciando una instancia de Web Proxy Server con la opción `-version`:

```
WebProxyServer-base/proxy-admserv/start -version
```

Consulte la [Tabla 13-4 en la página 268](#) para obtener los valores de salida.

Tareas posteriores a la actualización

No hay tareas posteriores a la actualización, además de las descritas en “[Procedimiento de actualización \(Solaris\)](#)” en la [página 270](#) y en “[Procedimiento de actualización \(Linux\)](#)” en la [página 271](#).

Deshacer la actualización (Solaris)

En esta sección, se describen diversas consideraciones que afectan al procedimiento que permite deshacer la actualización de Web Proxy Server, además de una descripción del propio procedimiento.

Consideraciones sobre la anulación de la actualización (Solaris)

El procedimiento para deshacer la actualización a la Versión 5 de Web Proxy Server es similar al procedimiento de actualización a esta versión, sólo que en el orden inverso.

Procedimiento de anulación de la actualización (Solaris)

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Detenga todas las instancias de Web Proxy Server y del servidor de administración que se estén ejecutando.

`WebProxyServer-base/proxy-instanceName/stop`

`WebProxyServer-base/proxy-admserv/stop`

3. Elimine las revisiones que aparecen en la [Tabla 13-5 en la página 269](#).

`patchrm patch_ID`

4. Reinicie las instancias de Web Proxy Server que se detuvieron en el [Paso 2](#).

`WebProxyServer-base/proxy-instanceName/start`

Actualización de Web Proxy Server desde la Versión 3.6

En esta sección se incluye información sobre la actualización de Web Proxy Server de la Versión 3.6 a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 3.6 de Web Proxy Server](#)

Introducción

Al actualizar Web Proxy Server a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** Para realizar la actualización, se debe utilizar el programa de instalación de Java ES para instalar Web Proxy Server en un directorio diferente del directorio de la versión 3.6. A continuación, se debe utilizar el servidor de administración de Web Proxy Server para migrar los valores de configuración (aunque no el contenido de la caché) de la Versión 3.6 a la Versión 5.
- **Dependencias de actualización.** La instalación de los componentes compartidos se realiza automáticamente mediante el programa de instalación de Java ES cuando se actualiza Web Proxy Server a la Versión 5.
- **Compatibilidad con versiones anteriores.** La Versión 5 de Web Proxy Server es compatible con la Versión 3.6, aunque se deben volver a compilar los complementos desarrollados mediante la interfaz NSAPI admitida por la Versión 3.6 en la interfaz NSAPI compatible con la Versión 5.
- **Anulación de la actualización.** Para deshacer la actualización a la Versión 5 de Web Proxy Server, se debe restablecer la Versión 3.6, que no ha sido modificada por el proceso de actualización.
- **Problemas de plataforma.** El enfoque de actualización de Web Proxy Server es igual en todas las plataformas Solaris. Sin embargo, no se admite la Versión 3.6 en las plataformas Linux.

Actualización de la Versión 3.6 de Web Proxy Server

En esta sección, se proporciona una visión general acerca de cómo realizar la actualización de Web Proxy Server a Java ES Versión 5. Anteriormente, Web Proxy Server no era compatible con la plataforma Linux. Por lo tanto, la actualización de Web Proxy Server a Java ES Versión 5 sólo se puede realizar en la plataforma Solaris. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 3.6 Web Proxy Server](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización de la Versión 3.6](#)

Tareas previas a la actualización

Antes de actualizar Web Proxy Server, debe realizar las tareas siguientes:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Web Proxy Server](#)
- [Copia de seguridad de los datos de Web Proxy Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Web Proxy Server, introduzca el siguiente comando:

```
WebProxyServer-base/proxy-serverid/start -version
```

Tabla 13-7 Resultados de la verificación de la versión de Web Proxy Server

Versión de Java ES	Número de versión de Web Proxy Server
Versión 3.6, no asociada a ninguna versión de Java ES	3.6
Versión 4	4.0.1
Componente de producto de la	4.0.4

Actualización de las dependencias de Web Proxy Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Sin embargo, el programa de instalación de Java ES utilizado para actualizar Web Proxy Server a la Versión 5 actualiza automáticamente todos los componentes compartidos de los que depende Web Proxy Server (consulte la [Tabla 1-7 en la página 49](#)).

Copia de seguridad de los datos de Web Proxy Server

La actualización de Web Proxy Server a la Versión 5 no modifica los datos de configuración de la Versión 3.6. Sin embargo, todos los cambios efectuados en la Versión 3.6 mediante la interfaz de administración deben guardarse antes de realizar la actualización.

Obtenga las contraseñas y la información de configuración necesarias

Para actualizar desde la Versión 3.6, debe conocer la ruta del directorio de instalación de la versión instalada.

Actualización de la Versión 3.6 Web Proxy Server

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Web Proxy Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización

Se pueden actualizar todas las instancias de Web Proxy Server que correspondan a la misma imagen instalada de Web Proxy Server. Sin embargo, la migración de los datos de configuración debe hacerse de forma independiente para cada instancia. Todas estas instancias deben cerrarse cuando se realice la migración para asegurarse de que no se produce ningún conflicto de puerto mientras se inicia la instancia migrada.

Procedimiento de actualización

El procedimiento que se describe a continuación hace referencia al software de Web Proxy Server que reside en el equipo en el que se va a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.
su -
2. Instale la Versión 5 de Web Proxy Server.
 - a. Ejecute el programa de instalación de Java ES desde la distribución de Java ES Versión 5.

- b.** Seleccione Web Proxy Server en la página de selección de componentes.
- c.** Seleccione la opción “Configurar ahora”.
- d.** Salga del programa de instalación de Java ES una vez completada la instalación.

3. Migre los valores de configuración a la nueva versión instalada.

Esta operación debe realizarse de forma independiente para cada instancia de Web Proxy Server.

- a.** Inicie el servidor de administración de Web Proxy Server.

WebProxyServer-base/proxy-admserv/start

- b.** Inicie sesión en la interfaz gráfica de administración.
- c.** Haga clic en la pestaña Servidor y, a continuación, en Migrar servidor.
- d.** Especifique la ruta del directorio de instalación de la Versión 3.6.
- e.** Seleccione la instancia que se va a migrar.
- f.** Haga clic en el botón Migrar.

Una vez realizada con éxito la migración, la pantalla muestra una lista de las configuraciones adicionales que deben realizarse manualmente. Proporciona los datos que se deben agregar y el archivo de configuración correspondiente.

Para obtener más información sobre la migración de los valores de configuración, consulte la *Sun Java System Web Proxy Server 4.0.4 Installation and Migration Guide* (<http://docs.sun.com/doc/819-5492>).

- 4.** Realice cualquier cambio adicional en la configuración de los que se especifican en el [Paso f](#).

Consulte *Sun Java System Web Proxy Server 4.0.4 Configuration File Reference* (<http://docs.sun.com/doc/819-5494>) para obtener más información.

Verificación de la actualización

Puede verificar la actualización de Web Proxy Server a la Versión 5 iniciando una instancia de Web Proxy Server con la opción `-version`:

WebProxyServer-base/proxy-serverid/start -version

Consulte la [Tabla 13-7 en la página 275](#) para obtener los valores de salida.

Tareas posteriores a la actualización

No hay tareas posteriores a la actualización, más allá de las descritas en [“Procedimiento de actualización” en la página 276](#).

Anulación de la actualización de la Versión 3.6

No se puede deshacer la actualización de Web Proxy Server a la Versión 5, descrita en [“Actualización de la Versión 3.6 Web Proxy Server” en la página 276](#). Sin embargo, puede restablecer la Versión 3.6, ya que el proceso de actualización a la Versión 5 no la ha modificado.

Access Manager

En este capítulo se describe cómo actualizar el software de Access Manager desde las versiones anteriores de Java ES a Java ES 5 (Versión 5): Sun Java System Access Manager 7.1.

Este capítulo proporciona una visión general de los problemas y los procedimientos de actualización de las diferentes rutas de actualización admitidas por la Versión 5 de Access Manager. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux:

- “Visión general de la actualización de Access Manager” en la página 282
- “Actualización de Access Manager desde Java ES Versión 4” en la página 290
- “Actualización de Access Manager desde Java ES Versión 3” en la página 315
- “Actualización de Access Manager desde Java ES Versión 2” en la página 320

NOTA Las ubicaciones de archivos de este capítulo se especifican en relación con dos rutas de directorio, a las que se denomina *AccessManager-base* y *AccessManagerConfig-base*. Debe haberse especificado, al menos, parte de estas rutas como directorio de instalación durante la instalación inicial de Access Manager. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado.

Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.

Tabla 14-1 Access Manager Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>AccessManager-base</i>	/opt/SUNWam	/opt/sun/identity
<i>AccessManagerConfig-base</i>	/etc/opt/SUNWam	/etc/opt/sun/identity

Visión general de la actualización de Access Manager

En esta sección se describen los siguientes aspectos generales de Access Manager que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Access Manager de Java ES Versión 5](#)
- [Guía de actualización de Access Manager](#)
- [Datos de Access Manager](#)
- [Estrategia de actualización para Access Manager](#)

NOTA	Las versiones de Access Manager anteriores a Java ES Versión 3 recibían el nombre de Identity Server. Por lo tanto, las referencias a Identity Server de este capítulo pertenecen a versiones anteriores del componente Java ES Access Manager.
-------------	---

Acerca de Access Manager de Java ES Versión 5

Access Manager de Java ES Versión 5 representa una versión inferior. Contiene una serie de soluciones a errores y mejoras con respecto a Access Manager de Java ES Versión 4, que era una versión superior. Entre las mejoras que ofrece la Versión 5 se encuentra una nueva función de supervisión basada en la estructura de supervisión de Java ES. Para más información sobre las mejoras de la Versión 5, consulte *Sun Java System Access Manager 7.1 Release Notes*, <http://docs.sun.com/doc/819-4683>.

Al igual que en la Versión 4, la Versión 5 de Access Manager admite varios depósitos de identidades o almacenes de datos de usuarios. Por lo tanto, el componente Access Manager de la Versión 5 no sólo admite un directorio LDAP como, por ejemplo, Directory Server, sino también otros formatos y protocolos de almacenamiento de datos.

En relación con los servicios de la interfaz, la consola de Access Manager se utiliza para configurar los nuevos servicios y depósitos de identidades de Access Manager.

Con el fin de ofrecer compatibilidad con otros componentes de Java ES de versiones anteriores, la Versión 5 puede ejecutarse en el modo tradicional, que admite los componentes de Java ES que dependen de los servicios de Access Manager de la Versión 3 (para más información, consulte [“Problemas de compatibilidad” en la página 286](#)).

Guía de actualización de Access Manager

La [Tabla 14-2](#) muestra las rutas de actualización compatibles de Access Manager para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 14-2 Rutas de actualización a Java ES 5 (Versión 5): Access Manager 7.1

Versión de Java ES	Access Manager Versión	Enfoque general	Reconfiguración necesaria
Versión 4	Sun Java System Access Manager 7.0 2005Q4	Actualización directa: Se realiza mediante la eliminación de la Versión 4 con una secuencia de comandos anterior a la actualización, y la instalación y reconfiguración completas de la Versión 5.	Datos de configuración JSP personalizados para la IU de autenticación y la consola de Access Manager Esquema de directorio
Versión 3	Sun Java System Access Manager 6.3 2005Q1	Actualización directa: Se realiza mediante la eliminación de la Versión 3 con una secuencia de comandos anterior a la actualización y, a continuación, la instalación y reconfiguración completas de la Versión 5.	Datos de configuración JSP personalizados para la IU de autenticación y la consola de Access Manager Esquema de directorio

Tabla 14-2 Rutas de actualización a Java ES 5 (Versión 5): Access Manager 7.1

Versión de			
Java ES	Access Manager Versión	Enfoque general	Reconfiguración necesaria
Versión 2	Sun Java System Identity Server 6.2 2004Q2 y también 6.2 SP1	Actualización directa: Se realiza mediante la eliminación de la Versión 2 con una secuencia de comandos anterior a la actualización y, a continuación, la instalación y reconfiguración completas de la Versión 5.	Datos de configuración JSP personalizados para la IU de autenticación y la consola de Access Manager Esquema de directorio
Versión 1	Sun ONE Identity Server 6.1	Sin actualización directa: Aunque puede actualizar primero a la Versión 3 utilizando los procedimientos descritos en la <i>Guía de migración y actualización de Java Enterprise System 2005Q1</i> , http://docs.sun.com/doc/819-0062 . A continuación, actualice de la Versión 3 a la Versión 5.	Datos de configuración JSP personalizados para la IU de autenticación y la consola de Access Manager Esquema de directorio
Versiones anteriores de Java ES	Sun ONE Identity Server 6.0, 6.0 SP 1 o iPlanet Directory Server Access Management Edition (DSAME) 5.1	Sin actualización directa.	

Datos de Access Manager

Access Manager, al igual que otros componentes Java ES, utiliza diversos tipos de datos para una actualización específica que es posible que se deban migrar a una versión actualizada. La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Access Manager.

Tabla 14-3 Uso de datos de Access Manager

Tipo de datos	Ubicación	Uso
Datos de configuración	<i>AccessManagerConfig-base/config/AMConfig.properties</i> <i>AccessManagerConfig-base/config/serverconfig.xml</i> Archivos JAR para los módulos de autenticación y personalizados <i>AccessManager-base/lib</i>	Configuración de Access Manager y su integración con un almacén de datos de servicios de fondo.
Archivos de configuración y control de acceso al contenedor web	Web Server 7.0 (Java ES Versión 5)Archivos <i>server.policy</i> y <i>server.xml</i> en <i>WebServer7Config-base/https-configName/config</i> Web Server 6.x (Java ES Versión 2, 3 y 4)Archivos <i>server.policy</i> y <i>server.xml</i> en <i>WebServer6-base/https-hostname/config</i> Application Server 8.x (Java ES Versión 3, 4 y 5):Archivos <i>server.policy</i> y <i>domain.xml</i> en <i>AppServer8Config-base/domains/domainName/config</i> Application Server 7.x (Java ES Versión 2):Archivos <i>server.policy</i> y <i>server.xml</i> en <i>AppServer7Config-base/domains/domainName/config</i> WebSphere y WebLogic: Los archivos de directivas y configuración respectivos se modifican al configurar Access Manager para estos contenedores web.	Configuración de la instancia del contenedor web de Access Manager
Datos de personalización (archivos JSP personalizados del contenedor web)	Admin Console: (Java ES Versión 2 y 3): <i>AccessManager-base/web-src/applications</i> Admin Console: (Java ES Versión 4 y 5): <i>AccessManager-base/web-src/services</i> IU de autenticación: <i>AccessManager-base/web-src/services</i>	Configuración de las interfaces de administración de Access Manager
Esquema de directorio Configuración de servicios Datos de usuario	Directory Server	Access Manager proporciona servicios de autenticación y autorización para los usuarios finales en función de los datos de directivas, usuarios y configuración de servicios almacenados en un directorio.

Tabla 14-3 Uso de datos de Access Manager

Tipo de datos	Ubicación	Uso
Datos de aplicación dinámicos	Ninguna	Access Manager no almacena de forma persistente datos de aplicación como, por ejemplo, el estado de la sesión.

Estrategia de actualización para Access Manager

La estrategia utilizada para la actualización de Access Manager depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Access Manager presentando una serie de problemas que pueden influir en el plan de actualización de Access Manager.

Problemas de compatibilidad

La Versión 5 de Access Manager es compatible con la Versión 4 de Access Manager. Sin embargo, la Versión 4 de Access Manager era una versión superior que rompía la compatibilidad con versiones anteriores, a no ser que se configurara para ejecutarse en modo tradicional. Del mismo modo, la Versión 5 de Access Manager, a no ser que se configure para ejecutarse en modo tradicional, no es compatible ni con la Versión 3 de Access Manager (ni con la Versión 4 de Access Manager ejecutándose en modo tradicional).

Además, la Versión 5 de Access Manager no es compatible con ningún modo de la Versión 2 de Access Manager; la versión 5 de Access Manager no puede interactuar con la Versión 2 de Access Manager SDK, ni *viceversa*.

Cuando se configura la Versión 5 de Access Manager para que se ejecute en el modo de dominio más reciente, admite varios depósitos de identidades y protocolos de almacenamiento de datos. Los datos de directorio tienen que migrarse a una nueva estructura para que sean compatibles con la operación en modo de dominio. Además, el modo de dominio no es compatible con otros componentes de Java ES como, por ejemplo, componentes de Portal Server o Sun Java Communications Suite, como Communications Express o Messaging Server, entre otros.

Sin embargo, cuando la Versión 5 de Access Manager se configura para que sea ejecutada en el modo tradicional (salvo raras excepciones que se pueden consultar en las *Sun Java System Access Manager 7.1 Release Notes*, <http://docs.sun.com/doc/819-4683>), es compatible con la Versión 3 de Access Manager y con los datos de directorio correspondientes.

El modo tradicional es necesario para obtener compatibilidad con otros componentes de Java ES, así como con las versiones antiguas de los agentes de directivas de Access Manager, que no pueden interactuar con Access Manager en el modo de dominio. Esta incompatibilidad supone un importante problema de actualización y, en la mayoría de las implementaciones de Java ES, implica la actualización obligatoria de Access Manager al modo tradicional de la Versión 5.

Aunque se haya configurado para ejecutarse en el modo tradicional, el componente de Access Manager de la Versión 5 es incompatible con el de la Versión 3 o con componentes anteriores de Sun Java Communications Suite. Si Access Manager se actualiza a la Versión 5, entonces también se deben actualizar a esta versión la Versión 3 o anteriores de Delegated Administrator para la configuración de usuarios de Messaging Server y Calendar Server. Sin embargo, no es necesario actualizar Messaging Server ni Calendar Server a la Versión 5.

La Versión 5 de la consola de Access Manager, al igual que la Versión 4 de la consola, admite tanto el modo tradicional como el modo de dominio. Sin embargo, si ha configurado Access Manager para que se ejecute en el modo tradicional, puede seguir utilizando la consola que sólo admite el modo tradicional distribuida con la Versión 2 y la Versión 3.

Dependencias de Access Manager

Las dependencias de Access Manager con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Access Manager. Por ejemplo, los cambios en las interfaces o las funciones de Access Manager pueden requerir las versiones actualizadas de los componentes de los que depende Access Manager. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Access Manager presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Access Manager presenta relaciones de dependencia con componentes compartidos específicos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). La actualización de Access Manager puede depender de las versiones actualizadas de estos componentes compartidos.

- **Contenedor web.** Access Manager tiene una dependencia obligatoria de los servicios de contenedores web proporcionados por Java ES Web Server, Java ES Application Server o contenedores web de terceros (de Weblogic y WebSphere). La actualización de Access Manager puede requerir que los JSP personalizados de la consola de Access Manager o de la IU de autenticación se migren al entorno actualizado de Access Manager.
- **Directory Server.** Access Manager tiene una dependencia obligatoria de Directory Server, utilizado para almacenar los datos de configuración y los datos del usuario. Por lo tanto, es posible que las actualizaciones de Access Manager necesiten las extensiones del esquema de directorio.

Escenarios de actualización del contenedor web

Access Manager puede implementarse en un contenedor web proporcionado por Web Server o Application Server. Por lo tanto, la actualización de Access Manager a la Versión 5 puede complicarse debido a la posibilidad de tener que actualizar también a la Versión 5 el contenedor web en el que se ha implementado. En este sentido, hay una serie de escenarios posibles de actualización del contenedor web, que se enumeran en la siguiente tabla.

Tabla 14-4 Escenarios de actualización del contenedor web para la actualización de Access Manager

Escenario	Contenedor web en el que se ha implementado originalmente Access Manager	Contenedor web en el que se ha implementado Access Manager después de la actualización	Rutas de actualización pertinentes de Access Manager : actualización desde
Escenario 1	Web Server 6.x	Web Server 6.x	Versión 2 Versión 3 Versión 4
Escenario 2	Web Server 6.x	Web Server 7.0	Versión 2 Versión 3 Versión 4
Escenario 3	Application Server 8.1	Application Server 8.1	Versión 3 Versión 4
Escenario 4	Application Server 8.1	Application Server 8.2	Versión 3 Versión 4
Escenario 5	Application Server 7x	Application Server 8.2	Versión 2

Tenga en cuenta que al actualizar Access Manager (por ejemplo, cuando utilice la secuencia de comandos `amconfig`) debe proporcionar los valores adecuados al escenario de actualización tal y como se indica en la [Tabla 14-4](#), especialmente cuando haya una versión superior de actualización del contenedor web.

Actualización de Access Manager desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Access Manager desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5). En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización completa de la Versión 4 de Access Manager](#)
- [Actualización de varias instancias](#)
- [Actualización sólo de Access Manager SDK de la Versión 4](#)

Introducción

Al actualizar Access Manager de Java ES Versión 4 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque general de actualización.** Para efectuar la actualización, se deben eliminar las versiones anteriores de archivos binarios e instalar la Versión 5. Se proporciona la secuencia de comandos `ampre71upgrade` para eliminar la Versión 4 y, a continuación, se utiliza el programa de instalación de Java ES para instalar la Versión 5. Después, se utiliza la secuencia de comandos `amconfig` para volver a configurar Access Manager y el esquema de directorio se migra mediante la secuencia de comandos `amupgrade`.
- **Dependencias de actualización.** Access Manager presenta relaciones de dependencia con varios componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Todos estos componentes se actualizan automáticamente a la Versión 5 mediante el programa de instalación de Java ES cuando realice una actualización de Access Manager. Esto incluye compatibilidad con la nueva estructura de supervisión de Java ES, que requiere varios componentes compartidos que no eran requeridos por la Versión 4 de Access Manager.

Además, el componente Access Manager de la Versión 5 depende de Directory Server y de Web Server (o de Application Server o contenedores web de terceros), tal y como se describe en [“Dependencias de Access Manager” en la página 287](#). Sin embargo, estas dependencias de actualización son leves, por lo que la actualización de estos componentes es opcional en relación con la actualización de Access Manager a la Versión 5.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Access Manager es compatible con la Versión 4, pero no es compatible con versiones anteriores de Access Manager (consulte [“Problemas de compatibilidad” en la página 286](#)).
- **Anulación de la actualización.** No existe ninguna utilidad para deshacer la actualización de Access Manager. De hecho, el número de reconfiguraciones necesarias para restablecer Access Manager a su estado original hacen imposible la anulación de la actualización. El mejor enfoque para la anulación es crear una instalación paralela utilizando las copias de seguridad de los archivos de configuración y comprobar esta instalación paralela antes de realizar la actualización. Esto le permite restablecer la instalación paralela si fuera necesario.
- **Problemas de plataforma.** El enfoque general de actualización de Access Manager es idéntico tanto para el sistema operativo Solaris como para Linux. Los procedimientos descritos a continuación indican comandos o ubicaciones de archivos específicos para cada plataforma cuando es pertinente.

Actualización completa de la Versión 4 de Access Manager

En esta sección se describe cómo realizar una actualización completa de Access Manager desde Java ES Versión 4 a Java ES Versión 5:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 4 de Access Manager](#)
- [Verificación de la actualización de Access Manager](#)
- [Tareas posteriores a la actualización](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Antes de actualizar Access Manager, debe realizar las tareas siguientes:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Access Manager](#)
- [Copia de seguridad de los datos de Directory Server](#)
- [Copia de seguridad de la información de configuración de la Versión 4 de Access Manager](#)

- [Copia de seguridad de los archivos personalizados del contenedor web](#)
- [Copia de seguridad de los archivos de depuración y registro de Access Manager de la Versión 4](#)
- [Copia de seguridad de los archivos de traducción personalizados](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Access Manager, utilice el siguiente comando:

```
AccessManager-base/bin/amadmin --version
```

Tabla 14-5 Resultados de la verificación de la versión de Access Manager

Versión de Java ES	Número de versión de Access Manager
Versión 2	6.2
Versión 3	6 2005Q1
Versión 4	7 2005Q4
Componente de producto de la	7.1

Actualización de las dependencias de Access Manager

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5. Access Manager presenta fuertes relaciones de dependencia con varios componentes compartidos (consulte la [Tabla 1-7 en la página 49](#)).

Si decide actualizar las dependencias de los componentes de productos de Access Manager, tiene que seguir los pasos que vienen a continuación (omitiendo cualquiera que ya se haya actualizado), antes de que actualice Access Manager. Normalmente, el programa de instalación de Java ES realiza automáticamente la actualización de los componentes compartidos.

- 1. Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación de Java ES actualiza automáticamente todos los componentes compartidos que requiere Access Manager cuando realiza una actualización a la Versión 5 de Access Manager.

2. **Directory Server (dependencia leve de actualización).** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [Capítulo 5, “Directory Server” en la página 107](#).
3. **Software de contenedor web (dependencia leve de actualización).** Las instrucciones para actualizar Web Server o Application Server están disponibles en el [Capítulo 7, “Web Server” en la página 141](#) y en el [Capítulo 11, “Application Server” en la página 219](#), respectivamente.

Si no se actualiza el software del contenedor web antes que Access Manager, el proceso de actualización (mediante la secuencia de comandos `amconfig`) configurará e implementará de nuevo Access Manager en el contenedor web existente.

Copia de seguridad de los datos de Directory Server

El proceso de actualización de Access Manager utiliza secuencias de comandos que modifican el esquema de Directory Server. Por tanto, antes de llevar a cabo la actualización de Access Manager, realice una copia de seguridad de los datos de Directory Server utilizando la consola de Directory Server o una utilidad de línea de comandos como `db2bak`. Puede utilizar `db2ldif` para realizar una copia de seguridad del esquema de Access Manager y del árbol de información de directorio (DIT).

Para más información sobre cómo realizar una copia de seguridad de Directory Server, consulte la *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

Copia de seguridad de la información de configuración de la Versión 4 de Access Manager

Debido a que la reconfiguración del software de Access Manager de la Versión 5 requiere la reconfiguración de la Versión 4, es importante realizar una copia de seguridad de los archivos de configuración en una ubicación conocida. Debería realizarse una copia de seguridad de los siguientes archivos:

- El archivo `AMConfig.properties`
AccessManagerConfig-base/config/AMConfig.properties
- El archivo `serverconfig.xml`
AccessManagerConfig-base/config/serverconfig.xml
- Archivos de configuración del contenedor web:
 - Para Web Server: consulte la ubicación de los archivos `server.policy` y `server.xml` en la [Tabla 14-3 en la página 285](#)

- Para Application Server: consulte la ubicación de los archivos `server.policy` y `domain.xml` en la [Tabla 14-3 en la página 285](#)
- Para los contenedores web de otros fabricantes: los archivos de configuración adecuados
- Archivos JAR para los módulos de autenticación y personalizados.

AccessManager-base/lib

Copia de seguridad de los archivos personalizados del contenedor web

Si tiene archivos personalizados del contenedor web relacionados con Access Manager, debería realizar una copia de seguridad de ellos. Entre las personalizaciones, se puede incluir las siguientes:

- Páginas JSP de la consola de Access Manager personalizadas:
 - Consola en modo tradicional o de dominio (distribuida con la Versión 4 de Java ES)
AccessManager-base/web-src/services
 - Consola que sólo admite el modo tradicional (distribuida con la Versión 2 y 3 de Java ES)
AccessManager-base/web-src/applications
- Páginas JSP de la IU de autenticación personalizadas.
AccessManager-base/web-src/services
- Archivos XML personalizados.
AccessManagerConfig-base/config/xml/

SUGERENCIA Anote las personalizaciones para que pueda volver a aplicarlas utilizando el código del que se ha realizado una copia de seguridad después de la actualización de Access Manager.

Copia de seguridad de los archivos de depuración y registro de Access Manager de la Versión 4

Con el fin de analizar la información del sistema, es recomendable realizar una copia de seguridad de los archivos de depuración y registro para que no se pierdan. Estos archivos se encuentran en las siguientes ubicaciones:

- Archivos de depuración
/var/AccessManager-base/debug

- Los archivos de registro.
/var/AccessManager-base/logs

Copia de seguridad de los archivos de traducción personalizados

Si ha realizado alguna personalización de los archivos traducidos instalados por el programa de instalación de Java ES o ha añadido un nuevo idioma de traducción que no se instala con el programa de instalación de Java ES, entonces tiene que realizar una copia de seguridad de estas personalizaciones. Entre las personalizaciones, se pueden incluir las siguientes:

- Traducción personalizada de la interfaz de usuario de Access Manager
*AccessManager-base/locale/*_Locale.properties*
- Páginas JSP de la IU de autenticación personalizadas
AccessManager-base/web-src/services/config/auth/default_Locale
- Traducciones personalizadas de la ayuda online
AccessManager-base/web-src/services/html/Locale

Obtenga las contraseñas y la información de configuración necesarias

Para actualizar Access Manager, debe proporcionar información de configuración específica, incluyendo:

- Id. de usuario del administrador y contraseña de Access Manager
- Id. de usuario y contraseña de LDAP
- Nombre y contraseña de Directory Manager para la instancia de Directory Server que esté utilizando Access Manager

Actualización de la Versión 4 de Access Manager

La actualización del software de Access Manager a Java ES Versión 5 incluye procedimientos para volver a configurar Access Manager y migrar los datos de Access Manager.

Resumen de la actualización

El proceso de actualización de Access Manager consta de los siguientes pasos:

1. [Actualización del software de acceso móvil de Access Manager.](#)
2. [Elimine la aplicación Access Manager de Java ES Versión 4.](#) Utilice la secuencia de comandos `ampre71upgrade` .

3. Si la actualización a la Versión 5 tiene que adaptarse a la configuración regional, elimine los paquetes traducidos de la Versión 4. Este paso tiene que llevarse a cabo manualmente.
4. Instale la versión de Access Manager de Java ES Versión 5. Utilice el programa de instalación de Java ES con la opción Configurar más tarde.
5. Vuelva a personalizar los archivos JSP para Access Manager.
6. Anule la implementación de Access Manager y vuelva a configurarlo e implementarlo en un contenedor web. Utilice la secuencia de comandos amconfig.
7. Actualice la estructura y el esquema de directorio. Utilice la secuencia de comandos amupgrade.

Estos pasos se describen en los siguientes procedimientos.

Procedimiento de actualización

1. Actualización del software de acceso móvil de Access Manager.

El software de acceso móvil de Access Manager debe actualizarse mediante la aplicación de revisiones en la Versión 4. Las revisiones necesarias se muestran en la siguiente tabla:

Tabla 14-6 Revisiones¹ de actualización del software de acceso móvil de Access Manager

Descripción	Id. de revisión: Solaris 9 y 10	Id. de revisión: Linux
Software de Mobile Access	119530-05 (SPARC)	119532-05
	119531-05 (x86)	• sun-identity-mobileaccess-6.2-25.3.i386.rpm • sun-identity-mobileaccess-config-6.2-25.3.i386.rpm

1. Los números de revisiones suponen la revisión mínima necesaria para actualizar a Java ES Versión 5. Si aparecen nuevas revisiones, utilícelas en lugar de las que aparecen en la tabla.

- a. Obtenga las revisiones necesarias mediante los números de revisión que aparecen en la [Tabla 14-6](#).

Las revisiones pueden descargarse en /tmp desde:
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

- b. Lleve a cabo cualquiera de los procedimientos previos a la revisión indicados en los archivos de revisión README.
- c. Obtenga los valores de los siguientes parámetros que le solicitará la revisión:

Tabla 14-7 Parámetros de revisión de Mobile Access

Parámetro	Valor
DN de administrador de directorios	valor predeterminado: cn=Directory Manager
Contraseña de administrador de directorios	

- d. Aplique las revisiones que aparecen en la [Tabla 14-6](#).

En Solaris:

```
patchadd /tmp/patch_ID
```

En Linux:

```
./update
```

Lleve a cabo cualquiera de los procedimientos posteriores a la revisión indicados en los archivos de revisión README.

2. Elimine la aplicación Access Manager de Java ES Versión 4.
 - a. Inicie sesión como root en el equipo en el que resida la Versión 4 de Access Manager o conviértase en superusuario.

su -
 - b. Cambie el directorio al directorio *os_arch/Product/identity_svr/Tools* en la distribución de Java ES Versión 5, donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.
 - c. Obtenga los valores de los siguientes parámetros que le solicitará la secuencia de comandos *ampre71upgrade* :

Tabla 14-8 Parámetros de configuración de Access Manager *ampre71upgrade*

Parámetro	Valor
Host de Directory Server	Defina el nombre completo: <i>hostname.domain</i>
Puerto de Directory Server	Especifique un número de puerto que no sea SSL ¹ Valor predeterminado: 389

Tabla 14-8 Parámetros de configuración de Access Manager ampre71upgrade

Parámetro	Valor
DN de administrador de nivel superior	Valor predeterminado: uid=amadmin,ou=People,default_org_DN
Contraseña del administrador de nivel superior:	
Directorio de almacenamiento de las copias de seguridad de los archivos	Valor predeterminado: <i>AccessManager-base</i>

1. El proceso previo a la actualización no se completará satisfactoriamente si especifica un puerto SSL de Directory Server como, por ejemplo, el valor SSL predeterminado, 636.

- d. Asegúrese de que Directory Server se esté ejecutando. De lo contrario, inícielo.
- e. Ejecute la secuencia de comandos ampre71upgrade.

./ampire71upgrade

La secuencia de comandos realiza una copia de seguridad de los archivos de configuración de Access Manager y elimina los paquetes de la Versión 4 básica (los paquetes traducidos deben eliminarse manualmente según lo indicado en el [Paso 3](#)).

- 3. Si la actualización a la Versión 5 tiene que adaptarse a la configuración regional, elimine los paquetes traducidos de la Versión 4.

La secuencia de comandos ampre71upgrade ejecutada anteriormente en el [Paso 2](#) no elimina los paquetes traducidos, por lo que tendrá que eliminarlos manualmente como se indica a continuación.

En Solaris:

- a. Busque los paquetes traducidos.

```
pkginfo | grep SUNWaml  
pkginfo | grep SUNWamclnt  
pkginfo | grep SUNWamdistauth
```
- b. Elimine cualquier paquete traducido que haya encontrado en el [Paso a](#) mencionado anteriormente.

```
pkgrm SUNWamlLocale  
pkgrm SUNWamclntLocale  
pkgrm SUNWamdistauthLocale
```

En Linux:

- a. Busque los RPM traducidos.

```
rpm -qa | grep sun-identity-sdk-*
rpm -qa | grep sun-identity-clientsdk-*
rpm -qa | grep sun-identity-distauth-*
```

- b. Elimine cualquier RPM traducido que haya encontrado en el [Paso a](#) mencionado anteriormente.

```
rpm -e sun-identity-sdk-Locale-*
rpm -e sun-identity-clientsdk-Locale-*
rpm -e sun-identity-distauth-Locale-*
```

4. Instale la versión de Access Manager de Java ES Versión 5.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES en el equipo que aloje la Versión 4 de Access Manager.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción `installer -nodisplay` para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b. Seleccione Access Manager en la página de selección de componentes.
- c. Especifique el mismo directorio de instalación en el que se haya instalado la Versión 4.
- d. Seleccione la opción Configurar más tarde.
- e. Si fuera necesario, seleccione la opción para instalar paquetes traducidos.
- f. Una vez completada la instalación, salga del programa de instalación de Java ES.

5. Vuelva a personalizar los archivos JSP para Access Manager.

Vuelva a aplicar las personalizaciones de la Versión 4 a los archivos JSP de la consola de Access Manager y a la interfaz de usuario de autenticación (IU) que guardó en “[Copia de seguridad de los archivos personalizados del contenedor web](#)” en la [página 294](#).

A continuación, copie los archivos JSP personalizados en los directorios correspondientes:

- Consola en modo tradicional o de dominio de Access Manager
AccessManager-base/web-src/services/console
- Consola de Access Manager que sólo admite el modo tradicional
AccessManager-base/web-src/applications/console
- IU de autenticación:
AccessManager-base/web-src/services/config/auth/default o
AccessManager-base/web-src/services/config/auth/default_Locale
(donde *Locale* es un indicador de configuración regional como, por ejemplo, *ja*)

Para obtener más información, consulte la *Sun Java System Access Manager 7.1 Developer's Guide*, <http://docs.sun.com/doc/819-4675>.

6. Anule la implementación de Access Manager y vuelva a configurarlo e implementarlo en un contenedor web.

Configure Access Manager para el contenedor web específico ejecutando la secuencia de comandos `amconfig`. La secuencia de comandos `amconfig` (y el archivo de entrada de plantilla asociado, `amsamplesilent`) reside en el siguiente directorio:

AccessManager-base/bin

Para más información acerca de la secuencia de comandos `amconfig` y el archivo de plantilla `amsamplesilent`, consulte la *Sun Java System Access Manager 7.1 Administration Guide*, <http://docs.sun.com/doc/819-4670>.

Lleve a cabo los siguientes pasos para volver a configurar e implementar Access Manager en el contenedor web:

- a. Si decide actualizar el software del contenedor web como se describe en “[Actualización de las dependencias de Access Manager](#)” en la [página 292](#), asegúrese de que se haya completado la actualización.
- b. Asegúrese de que se está ejecutando en el contenedor web la instancia administrativa y lo hace en un modo que admita la secuencia de comandos `amconfig`, tal y como se indica en la siguiente tabla.

Tabla 14-9 Modos de Administrative Server admitidos por amconfig

Contenedor Web	Modo admitido	Número de puerto predeterminado
Application Server (8.x): Java ES Versión 3, 4 y 5	SSL (seguro) no SSL	4849
Web Server (7.0): Java ES Versión 5	SSL (seguro)	8989
Web Server (6.x): Java ES Versión 2, 3 y 4	no SSL	8888

- c. Si el contenedor web se está ejecutando en modo SSL, asegúrese de que los certificados SSL del contenedor no hayan caducado y sigan siendo válidos.
- d. Si Access Manager se implementa en la Versión 5 de Web Server, deshabilite todos los componentes de Java ES que dependan de Access Manager y que se estén ejecutando en la misma instancia que Access Manager.

Lo más probable es que sean componentes de Portal Server o Sun Java Communications Suite como, por ejemplo, Communications Express, Instant Messaging o Delegated Administrator.

El procedimiento es el siguiente:

- I. Inicie sesión como administrador en `https://host:8989`
 - II. Vaya a Editar servidor virtual.
 - III. Seleccione la pestaña Web Applications.
 - IV. Compruebe todas las aplicaciones que dependan de Access Manager.
 - V. Haga clic en Deshabilitar.
 - VI. Haga clic en "Guardar".
 - VII. Haga clic en deployment pending | Deploy Config. (implementación pendiente | Configuración de la implementación).
- El cambio en la configuración se propagará a la instancia de Web Server.
- e. Compruebe que Directory Server y el contenedor web adecuado se estén ejecutando.

- f. Cree un archivo de entrada `amconfig` basado en el archivo de entrada de plantilla `amsamplesilent`:

```
cp amsamplesilent config-file
```

(En los pasos siguientes, *config-file* se supone que reside en el mismo directorio que `amsamplesilent`.)

- g. Establezca los parámetros de configuración en *config-file*.

Todos los parámetros deben establecerse correctamente. Algunos de los valores pueden migrarse desde el archivo `AMConfig.properties`, aunque otros son más específicos del proceso de actualización, como se muestra en la siguiente tabla.

Tabla 14-10 Parámetros de configuración de Access Manager `amconfig`

Parámetro	Valor
Parámetros de actualización	
DEPLOY_LEVEL	Establézcalo en 26 (para la anulación de la implementación) ó en 1 (para la reconfiguración e implementación)
DIRECTORY_MODE	Establézcalo en 5
AM_REALM ¹	Establézcalo en disabled (si el modo tradicional está habilitado) Establézcalo en enabled (si el modo de dominio está habilitado) Valor predeterminado: enabled
JAVA_HOME	Establézcalo en el directorio de JDK de la Versión 5: /usr/java/jdk1.5.0_04/
WEB_CONTAINER	Establézcalo en WS para Web Server 7.x Establézcalo en WS6 para Web Server 6.x Establézcalo en AS8 para Application Server 8.x Establézcalo en WAS5 para IBM WebSphere 5.x Establézcalo en WL8 para BEA WebLogic 8.x y rellene solamente la sección correspondiente de <i>config-file</i> .
WS_INSTANCE (Si se utiliza Web Server 7.x como contenedor web)	Defina el nombre de la instancia de directorio de configuración para que distinga entre mayúsculas y minúsculas: <code>https-configNameI</code> El directorio está en la siguiente ruta: <code>WebServer7Config-baseIhttps-configNameI</code>

Tabla 14-10 Parámetros de configuración de Access Manager `amconfig`

Parámetro	Valor
WS61_INSTANCE (Si se utiliza Web Server 6.x como contenedor web)	Defina el nombre de la instancia de directorio de configuración para que distinga entre mayúsculas y minúsculas: <code>https-instanceName</code> El directorio está en la siguiente ruta: <code>WebServer6-base/https-instanceName/</code>
AS81_INSTANCE (Si se utiliza Application Server 8.x como contenedor web)	Establézcalo en Application Server 8.x <code>instanceName</code> Valor predeterminado: servidor
AS81_INSTANCE_DIR (Si se utiliza Application Server 8.x como contenedor web)	Establézcalo en el directorio de dominio de Application Server 8.x para la instancia, cuyo valor predeterminado es <code>AppServer8Config-base/domains/domain1</code>
AS81_DOCS_DIR (Si se utiliza Application Server 8.x como contenedor web)	Establezca el valor en el directorio de dominio de Application Server 8.x para la instancia, cuyo valor predeterminado es <code>AppServer8Config-base/domains/domain1/docroot</code>

Migrados desde `AMConfig.properties`

SERVER_PROTOCOL	<code>com.iplanet.am.server.protocol</code>
SERVER_PORT	<code>com.iplanet.am.server.port</code>
SERVER_HOST	<code>com.iplanet.am.server.host</code>
DS_HOST	<code>com.iplanet.am.directory.host</code>
DS_PORT	<code>com.iplanet.am.directory.port</code>
ROOT_SUFFIX ²	<code>com.iplanet.am.defaultOrg</code>
CONSOLE_DEPLOY_URI	<code>com.iplanet.am.console.deploymentDescriptor</code>
SERVER_DEPLOY_URI	<code>com.iplanet.am.services.deploymentDescriptor</code>
PASSWORD_DEPLOY_URI	<code>com.sun.identity.password.deploymentDescriptor</code>
AM_ENC_PWD ²	<code>am.encryption.pwd³</code>

1. Para más información sobre el modo tradicional y el de dominio, consulte [“Problemas de compatibilidad” en la página 286](#).
2. El valor de este parámetro tiene que ser el mismo que el de la versión anterior de Access Manager.
3. Cuando se implementan Access Manager y Access Manager SDK, el valor de esta propiedad debe ser el mismo para la instancia de Access Manager y su instancia asociada de Access Manager SDK.

Para los demás parámetros, especifique los mismos valores utilizados en la configuración de la Versión 4 que está actualizando, a menos que cambie el contenedor web o las contraseñas. Por ejemplo, si ha actualizado Web Server a la Versión 5, proporcione los siguientes valores:

Tabla 14-11 Parámetros de amconfig: Versión 5Web Server

Parámetro	Valor
WS_CONFIG	El nombre de configuración de Web Server: <i>configName</i>
WS_INSTANCE	<i>https-configName</i>
WS_HOME	<i>WebServer7Config-base</i>
WS_PROTOCOL	http o https
WS_HOST	Nombre de host completo en el que se produce la escucha de conexiones de la instancia de Web Server
WS_PORT	Puerto en el que se produce la escucha de conexiones de la instancia de Web Server
WS_ADMINPORT	Puerto en el que se produce la escucha de conexiones de la administración de Web Server
WS_ADMIN	Id. de usuario del administrador de Web Server
WS_ADMINPASSWD	Contraseña de administrador de Web Server

- h. Ejecute amconfig para anular la implementación de Access Manager
Establezca el valor de DEPLOY_LEVEL de *config-file* en 26.

```
cd /AccessManager-base/bin
./amconfig -s AccessManager-base/bin/config-file
```

- i. Compruebe que se está ejecutando el contenedor de agentes común.

```
netstat -an | grep 11163

Si no se está ejecutando, inícielo.

/usr/sbin/cacaoadm start
```

- j. Ejecute `amconfig` para volver a configurar Access Manager e implementarlo en un contenedor web.

Establezca el valor de `DEPLOY_LEVEL` de *config-file* en 1.

```
cd /AccessManager-base/bin
./amconfig -s AccessManager-base/bin/config-file
```

7. Actualice la estructura y el esquema de directorio.

La Versión 5 de Access Manager coexiste con la estructura de directorio de la Versión 4, aunque ésta deba modificarse para que pueda admitir las funciones de la Versión 5. Actualice la estructura y el esquema de directorio de Access Manager a la Versión 5 ejecutando la secuencia de comandos `amupgrade`, que está instalada en el siguiente directorio:

- o *En Solaris:*
AccessManager-base/upgrade/scripts
 - o *En Linux:*
AccessManager_base/identity/upgrade/scripts
- a. Obtenga los valores de los siguientes parámetros que le solicitará la secuencia de comandos `amupgrade` :

Tabla 14-12 Parámetros de configuración de Access Manager `amupgrade`

Parámetro	Valor
Nombre completo de host de Directory Server	Defina el nombre completo: <i>nombrehost.dominio</i>
Puerto de Directory Server	Especifique un número de puerto que no sea SSL ¹ Valor predeterminado: 389
DN de administrador de directorios	Valor predeterminado: cn=Directory Manager
Contraseña del administrador de directorios	
DN de administrador de nivel superior	Valor predeterminado: <i>uid=amadmin,ou=People,default_org_DN</i>
Contraseña del administrador de nivel superior:	

Tabla 14-12 Parámetros de configuración de Access Manager amupgrade

Parámetro	Valor
Habilitar modo de dominio (Este valor de parámetro no se solicita cuando se actualiza desde la Versión 4 en modo de dominio).	Y/N: Yes (Sí) implica la activación del modo de dominio y la migración de los servicios de datos al nuevo árbol de dominio ² . No (valor predeterminado) implica que los servicios de datos permanecen en el modo tradicional.

- 1. Debe especificar un puerto SSL de Directory Server diferente del valor SSL predeterminado, 636.
- 2. Consulte el [“Migración al modo de dominio” en la página 308](#).

- b.** Ejecute la secuencia de comandosamupgrade.

```
cd AccessManager-base/upgrade/scripts
./amupgrade
```

Si la actualización se realiza con éxito, la secuencia de comandos muestra “Upgrade completed.”

- c.** Consulte el siguiente archivo de registro de actualización para obtener información sobre las extensiones del esquema de directorio:

```
En Solaris:
/var/sadm/install/logs/
    Sun_Java_System_Access_Manager_upgrade_dit_log.mmddhhmm

En Linux:
/var/log/Sun_Java_System_Access_Manager_upgrade_dit_log.mmddhhmm
```

- 8.** Habilite cualquier componente que estuviera deshabilitado en el [Paso d en la página 301](#).
- 9.** Reinicie el contenedor web en el que se haya implementado Access Manager.
- 10.** Inicie Access Manager.

Reinicie el contenedor web en el que se haya implementado Access Manager.

Verificación de la actualización de Access Manager

Una vez completado el proceso de actualización, compruebe que la actualización se ha realizado con éxito de la siguiente manera:

- 1.** Compruebe los paquetes de Access Manager con el siguiente comando:

AccessManager-base/bin/amadmin --version

Consulte la [Tabla 14-5 en la página 292](#) para obtener los valores de salida.

2. Para revisar el estado de la actualización, compruebe los siguientes archivos de registro del programa de instalación en el directorio `/var/sadm/install/logs`:
 - `Java_Shared_Component_Install.timestamp`
 - `Java_Enterprise_System_install.Atimestamp`
 - `Java_Enterprise_System_install.Btimestamp`
 - `Java_Enterprise_System_Summary_Report_install.timestamp`
3. Revise el estado de la migración de Access Manager comprobando si hay errores en la ventana terminal mientras se ejecuta la secuencia de comandos `amupgrade`.

Compruebe también el siguiente archivo de registro en el directorio `/var/sadm/install/logs` :

Sun_Java_System_Access_Manager_upgrade_dit_log.timestamp

4. Busque la existencia de errores en los archivos de resolución de problemas de Access Manager.

Los archivos se encuentran en la ubicación especificada en la propiedad `com.ipplanet.services.debug.directory` del archivo `AMConfig.properties`. Los valores predeterminados son:

En Solaris:

`/var/opt/SUNWam/debug`

En Linux:

`/var/opt/sun/identity/debug`

Tareas posteriores a la actualización

Tenga en cuenta los procedimientos posteriores a la actualización necesarios para abordar las siguientes situaciones:

- [Migración al modo de dominio](#)
- [Security Assertion Markup Language](#)
- [Actualización de revisiones](#)

Migración al modo de dominio

Si ha migrado al modo de dominio cuando actualizaba Access Manager a la Versión 5 (es decir, si al utilizar `amupgrade` para actualizar la estructura y el esquema de directorio, respondió Yes (Sí) para habilitar el modo de dominio), siga los pasos que se indican a continuación:

1. Abra el archivo `AccessManagerConfig-base/config/AMConfig.properties`.
2. Compruebe el valor de la siguiente propiedad:
`com.sun.identity.sm.ldap.enableProxy`
3. Si la propiedad no establece el valor en `false`, entonces establézcalo manualmente en `false`.

Security Assertion Markup Language

Si está utilizando el servicio Security Assertion Markup Language (SAML), deberá agregar y habilitar el módulo de autenticación SAML mediante la consola de Access Manager. Para obtener información sobre cómo crear una instancia del módulo de autenticación SAML, consulte la *Sun Java System Access Manager 7.1 Administration Guide* (<http://docs.sun.com/doc/819-4670>).

Actualización de revisiones

Después de la actualización tiene que descargarse, si existieran, las últimas revisiones de Access Manager 7.1 y seguir las instrucciones de revisión sobre cómo aplicar la revisión y llevar a cabo cualquier procedimiento de configuración posterior a ésta.

Anulación de la actualización

No se proporciona ninguna secuencia de comandos para restablecer Access Manager al estado anterior a la actualización. Este proceso debe realizarse manualmente utilizando los datos de Access Manager de los que se realizó una copia de seguridad como parte de las tareas previas a la actualización (consulte [“Copia de seguridad de los archivos de depuración y registro de Access Manager de la Versión 4” en la página 294](#)). El procedimiento para deshacer la actualización es poco práctico debido a su complejidad.

Un enfoque para la anulación es volver a realizar una instalación de la Versión 4 y migrar todas las copias de seguridad de los archivos de configuración a sus ubicaciones legítimas. Otra opción es la de crear un sistema paralelo antes de realizar la actualización, utilizando las copias de seguridad de los archivos de configuración y probando el sistema paralelo antes de intentar la actualización.

Actualización de varias instancias

En algunas arquitecturas de implementación, Access Manager se implementa en varios sistemas informáticos para proporcionar alta disponibilidad y escalabilidad.

A menudo es recomendable actualizar las instancias de Access Manager secuencialmente sin necesidad de interrumpir el servicio. En esta sección se describe el procedimiento que se sigue para llevar a cabo estas actualizaciones por turnos de Access Manager desde la Versión 4 a la Versión 5.

NOTA	Sin embargo, en esta versión, no se admite la actualización de varias instancias de Access Manager instaladas en el mismo host. Si tiene varias instancias en el mismo host, una vez actualizada la instancia principal, debe volver a crear las instancias adicionales.
-------------	--

La arquitectura de implementación que se muestra en la figura que aparece a continuación sirve para ilustrar el procedimiento de actualización por turnos:

Figura 14-1 Ejemplo de arquitectura de implementación de varias instancias de Access Manager



En esta arquitectura, se accede a varias instancias de Access Manager mediante un equilibrador de carga y estas instancias, a su vez, acceden a un directorio que está configurado para la repetición de varias réplicas principales (MMR). Aunque se pueden utilizar otros esquemas de repetición de Directory Server, MMR es una función representativa de los servicios de directorios escalables y de alta

disponibilidad. En la [Figura 14-1](#) se agrupan varias instancias de Access Manager y de Directory Server para facilitar la explicación del procedimiento de actualización. Access Manager 2, por ejemplo, es representativo desde la segunda instancia hasta la n de Access Manager.

El procedimiento que se sigue para llevar a cabo una actualización de Access Manager de la Versión 4 a la Versión 5 está basado en la siguiente interoperatividad: Las instancias de la Versión 5 de Access Manager y la Versión 4 de Access Manager pueden coexistir y ejecutarse simultáneamente en el mismo directorio, siempre que el esquema del directorio no se haya actualizado todavía a la Versión 5.

De ahí que para las instancias de Access Manager que señalan a una única instancia de Directory Server sea posible llevar a cabo una actualización por turnos, retrasando la actualización del esquema del directorio hasta que se hayan actualizado todas las instancias de Access Manager.

Puede llevar a cabo una actualización por turnos de Access Manager desde la Versión 4 a la Versión 5 siguiendo el siguiente procedimiento:

1. Realice una copia de seguridad de la información de configuración de todas las instancias de la Versión 4 de Access Manager.
2. Actualice Access Manager 1.

- a. Deshabilite Access Manager 1 en el equilibrador de carga.

Las solicitudes ya no se enrutarán a Access Manager 1.

- b. Actualice parcialmente Access Manager 1.

Actualice Access Manager tal y como se describe en [“Actualización de la Versión 4 de Access Manager” en la página 295](#), pero actualice la estructura y el esquema del directorio, como se describe en el [Paso 7 en la página 305](#).

- c. Habilite Access Manager 1 en el equilibrador de carga.

3. Actualice Access Manager 2 mediante Access Manager n.

Para mayor brevedad, al realizar los pasos posteriores Access Manager 2” significará Access Manager 2 hasta Access Manager n.

- a. Deshabilite Access Manager 2 en el equilibrador de carga.

Las solicitudes ya no se enrutarán a Access Manager 2.

b. Actualice parcialmente Access Manager 2.

Actualice todas las instancias de Access Manager tal y como se describe en [“Actualización de la Versión 4 de Access Manager” en la página 295](#), pero actualice la estructura y el esquema del directorio, como se describe en el [Paso 7 en la página 305](#).

c. Habilite Access Manager 2 en el equilibrador de carga.

Las solicitudes se volverán a enrutar a Access Manager 2.

4. Actualice la estructura y el esquema de directorio de Directory Server 1.

Utilice la secuencia de comandos `amupgrade` como se indica en el [Paso 7 en la página 305](#). Access Manager 1 seguirá funcionando porque el esquema de Directory Server 2 no se ha actualizado.

Actualización sólo de Access Manager SDK de la Versión 4

En algunas arquitecturas de implementación, el componente Access Manager SDK en uno o varios sistemas informáticos sin necesidad de instalar los otros componentes de Access Manager en dichos equipos. Access Manager SDK sirve como interfaz remota de Access Manager y debe volverse a configuración con el mismo modo operativo que Access Manager: el modo tradicional o de dominio.

Tanto Access Manager SDK, como la aplicación completa de Access Manager para la que sirve de interfaz remota, deben ser actualizadas a la Versión 5. Sin embargo, la Versión 5 de Access Manager es compatible con la Versión 4 de Access Manager SDK, por lo que Access Manager se actualizará por lo general en otros equipos antes que Access Manager SDK.

Como interfaz remota de Access Manager, no es necesario configurar SDK para acceder a Directory Server. Si Access Manager SDK se utiliza para obtener compatibilidad con un contenedor web, como Portal Server, que dependa de los servicios de contenedor web, Access Manager SDK debe configurarse para el contenedor web correspondiente. Sin embargo, Access Manager SDK también admite componentes que no sean web, por lo que no sería necesario ningún contenedor web.

El procedimiento de actualización de Access Manager SDK es un procedimiento secundario de la actualización completa de Access Manager, basado en las características mencionadas anteriormente.

En esta sección se describe cómo realizar la actualización sólo de Access Manager SDK de Java ES Versión 4 a Java ES Versión 5:

- [Tareas previas a la actualización](#)
- [Actualización del componente de Access Manager SDK de la Versión 4](#)
- [Verificación de la actualización de Access Manager SDK](#)
- [Anulación de la actualización](#)

Tareas previas a la actualización

Las tareas previas a la actualización de Access Manager SDK son las mismas que las del procedimiento completo de actualización de Access Manager (consulte [“Tareas previas a la actualización” en la página 291](#)), salvo que no se realizan aquellas tareas relacionadas con Directory Server y con las personalizaciones de la herramienta de administración de Access Manager. Entre las tareas previas necesarias para actualizar Access Manager SDK, se incluyen:

- [“Actualización de las dependencias de Access Manager” en la página 292](#)

Sin embargo, en Access Manager SDK no existe ninguna dependencia con Directory Server, aunque sí con el software del contenedor web, sólo si Access Manager SDK se ejecuta en un contenedor de este tipo.

- [“Copia de seguridad de la información de configuración de la Versión 4 de Access Manager” en la página 293](#)

Sin embargo, para Access Manager SDK, no es necesario realizar una copia de seguridad de los archivos de configuración del contenedor web si Access Manager SDK se ejecuta en un contenedor de este tipo.

- [“Copia de seguridad de los archivos de depuración y registro de Access Manager de la Versión 4” en la página 294](#)

Debe obtener el nombre de usuario y la contraseña de administración para acceder a estos archivos.

Actualización del componente de Access Manager SDK de la Versión 4

Los procedimientos de actualización de Access Manager SDK son los mismos que los de la actualización completa de Access Manager, salvo que no se realizan aquellos relacionados con la traducción, las personalizaciones JSP de la herramienta de administración de Access Manager y la migración del esquema de directorio.

1. Elimine la versión de Access Manager SDK de Java ES Versión 4.

Siga las instrucciones que aparecen en [“Elimine la aplicación Access Manager de Java ES Versión 4.” en la página 297](#), pero elimine solamente Access Manager SDK.

2. Instale la versión de Access Manager SDK de Java ES Versión 5.

Siga las instrucciones que aparecen en [“Instale la versión de Access Manager de Java ES Versión 5.” en la página 299](#), pero instale únicamente Access Manager SDK.

3. Vuelva a configurar Access Manager SDK.

Siga las instrucciones que aparecen en [“Anule la implementación de Access Manager y vuelva a configurarlo e implementarlo en un contenedor web.” en la página 300](#), pero establezca los parámetros DEPLOY_LEVEL de la siguiente forma:

- Si Access Manager SDK se configura para un contenedor web:
DEPLOY_LEVEL=4 (para actualizar el SDK y configurar el contenedor web)
- Si Access Manager SDK no se configura para un contenedor web:
DEPLOY_LEVEL=3 (para actualizar únicamente SDK)

Verificación de la actualización de Access Manager SDK

Existen tres formas de verificar la correcta actualización de Access Manager SDK:

- Ejecute Portal Server u otro componente que utilice Access Manager SDK como interfaz para Access Manager y compruebe que la autenticación funcione.
- Ejecute los ejemplos de Access Manager SDK proporcionados en la siguiente ubicación:

AccessManager-base/samples/sdk

- Compruebe el valor de la propiedad `com.ipplanet.am.version`, que se encuentra en el archivo `AMConfig.properties`:

AccessManagerConfig-base/config/AMConfig.properties

Anulación de la actualización

No se proporciona ninguna secuencia de comandos para restablecer Access Manager al estado anterior a la actualización. Este proceso debe realizarse manualmente utilizando los datos de Access Manager de los que se realizó una copia de seguridad como parte de las tareas previas a la actualización (consulte [“Copia de seguridad de los archivos de depuración y registro de Access Manager de la Versión 4” en la página 294](#)). El procedimiento para deshacer la actualización es poco práctico debido a su complejidad.

Un enfoque para la anulación es volver a realizar una instalación de la Versión 4 y migrar todas las copias de seguridad de los archivos de configuración a sus ubicaciones legítimas. Otra opción es la de crear un sistema paralelo antes de realizar la actualización, utilizando las copias de seguridad de los archivos de configuración y probando el sistema paralelo antes de intentar la actualización.

Actualización de Access Manager desde Java ES Versión 3

El procedimiento de actualización del componente Access Manager o Access Manager SDK de Java ES 2003Q1 (Versión 3) a la Versión 5 es parecido al procedimiento de actualización de la Versión 4 de Access Manager o Access Manager SDK a la Versión 5, a excepción de cómo se realizan las actualizaciones de varias instancias.

- [Actualización de la Versión 3 de Access Manager](#)
- [Actualización de varias instancias](#)

NOTA La Versión 5 de Access Manager es incompatible con algunos componentes de la Versión 3 de Sun Java Communications Suite. Si Access Manager se actualiza a la Versión 5, entonces también se deben actualizar a esta versión la Versión 3 o anteriores de Delegated Administrator para la configuración de usuarios de Messaging Server y Calendar Server. Sin embargo, no es necesario actualizar Messaging Server ni Calendar Server a la Versión 5.

Actualización de la Versión 3 de Access Manager

Para actualizar de la Versión 3 de Access Manager o de Access Manager SDK a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Access Manager desde Java ES Versión 4” en la página 290](#) y sustituya toda referencia a la Versión 4 por la Versión 3.

Actualización de varias instancias

En algunas arquitecturas de implementación, Access Manager se implementa en varios sistemas informáticos para proporcionar alta disponibilidad y escalabilidad.

A menudo es recomendable actualizar varias instancias de Access Manager secuencialmente sin necesidad de interrumpir el servicio. En esta sección se describe el procedimiento que se sigue para llevar a cabo estas actualizaciones por turnos de Access Manager desde la Versión 3 a la Versión 5.

NOTA Sin embargo, en esta versión, no se admite la actualización de varias instancias de Access Manager instaladas en el mismo host. Si tiene varias instancias en el mismo host, una vez actualizada la instancia principal, debe volver a crear las instancias adicionales.

La arquitectura de implementación que se muestra en la figura que aparece a continuación sirve para ilustrar el procedimiento de actualización por turnos:

Figura 14-2 Ejemplo de arquitectura de implementación de varias instancias de Access Manager



En esta arquitectura, se accede a varias instancias de Access Manager mediante un equilibrador de carga y estas instancias, a su vez, acceden a un directorio que está configurado para la repetición de varias réplicas principales (MMR). Aunque se pueden utilizar otros esquemas de repetición de Directory Server, MMR es una función representativa de los servicios de directorios escalables y de alta disponibilidad. En la [Figura 14-1](#) se agrupan varias instancias de Access Manager y de Directory Server para facilitar la explicación del procedimiento de actualización. Access Manager 2, por ejemplo, es representativo desde la segunda instancia hasta la n de Access Manager.

El procedimiento que se sigue para llevar a cabo una actualización de Access Manager de la Versión 3 a la Versión 5 está basado en la siguiente restricción: La Versión 5 de Access Manager *no* puede coexistir con la estructura de directorio de la Versión 3. Sin embargo, si se replican las instancias de Directory Server, como ocurre en la [Figura 14-2](#), entonces puede realizar una actualización por turnos siguiendo el procedimiento descrito a continuación:

1. Realice una copia de seguridad de la información de la configuración de todas las instancias de la Versión 3 de Access Manager.
2. Cambie la configuración de Access Manager 1.

- a. Configure Access Manager 1 para que señale a Directory Server 2 en lugar de a Directory Server 1.
- b. Reinicie Access Manager 1.

Access Manager 1 continuará administrando las solicitudes, mientras que desde Access Manager 2 hasta Access Manager n se actualizarán.

3. Actualice Access Manager 2 mediante Access Manager n.

Para mayor brevedad, al realizar los pasos posteriores Access Manager 2" significará Access Manager 2 hasta Access Manager n.

- a. Deshabilite Access Manager 2 en el equilibrador de carga.

Las solicitudes ya no se enrutarán a Access Manager 2.

- b. Actualice parcialmente Access Manager 2.

Actualice todas las instancias de Access Manager tal y como se describe en [“Actualización de la Versión 4 de Access Manager” en la página 295](#), pero actualice la estructura y el esquema del directorio, como se describe en el [Paso 7 en la página 305](#).

- c. Deshabilite la función MMR de Directory Server.
- d. Actualice la estructura y el esquema de directorio de Directory Server 1.

Utilice la secuencia de comandos `amupgrade` como se indica en el [Paso 7 en la página 305](#). Access Manager 1 seguirá funcionando porque el esquema de Directory Server 2 no se ha actualizado.

- e. Reinicie Access Manager 2.
- f. Habilite Access Manager 2 en el equilibrador de carga.

Las solicitudes se volverán a enrutar a Access Manager 2.

4. Actualice Access Manager 1.

- a.** Deshabilite Access Manager 1 en el equilibrador de carga.

Las solicitudes ya no se enrutarán a Access Manager 1.

- b.** Actualice parcialmente Access Manager 1.

Actualice Access Manager tal y como se describe en [“Actualización de la Versión 4 de Access Manager” en la página 295](#), pero actualice la estructura y el esquema del directorio, como se describe en el [Paso 7 en la página 305](#).

- c.** Habilite la función MMR de Directory Server.

Acaba de actualizarse el esquema (y los datos) de Directory Server 2.

- d.** Restaure la configuración de Access Manager 1 para que señale a Directory Server 1.

- e.** Reinicie Access Manager 1.

- f.** Habilite Access Manager 1 en el equilibrador de carga.

Las solicitudes se volverán a enviar a Access Manager 1, así como Directory Server a todas las otras instancias actualizadas de Access Manager.

Actualización de Access Manager desde Java ES Versión 2

El procedimiento de actualización de Access Manager de Java ES 2004Q2 (Versión 2) a la Versión 5 es parecido al procedimiento de actualización de Access Manager de la Versión 4 a la Versión 5, como se indica en las siguientes secciones:

- [Tareas previas a la actualización](#)
- [Actualización de la Versión 2 de Access Manager](#)
- [Actualización de varias instancias](#)

Del mismo modo, el procedimiento de actualización de Access Manager SDK de Java ES 2004Q2 (Versión 2) a la Versión 5 es el mismo que el procedimiento de actualización de la Versión 4 de Access Manager SDK a la Versión 5 (consulte [“Actualización sólo de Access Manager SDK de la Versión 4” en la página 311](#)), con excepciones similares. Access Manager SDK excluye de la actualización sólo los procedimientos relacionados con la traducción, las personalizaciones JSP de la herramienta de administración de Access Manager y la migración del esquema de directorio.

La Versión 2 de Access Manager SDK y la aplicación completa de la Versión 2 de Access Manager para la que sirve de interfaz remota, deben actualizarse a la Versión 5. No se admite la mezcla de componentes de la Versión 2 y la Versión 5. Por lo tanto, todas las instancias de la Versión 2 de Access Manager y de la Versión 2 de Access Manager SDK deben actualizarse a la Versión 5 en todos los equipos.

Tareas previas a la actualización

Antes de actualizar Access Manager, lleve a cabo los procedimientos descritos en [“Tareas previas a la actualización” en la página 291](#), con las siguientes excepciones y adiciones:

- [Actualización de las dependencias de Access Manager](#)
- [Actualice el esquema de directorio](#)
- [Vuelva a indexar el directorio](#)

Actualización de las dependencias de Access Manager

A diferencia del proceso de actualización de la Versión 4, entre las tareas previas a la actualización de la Versión 2 a la Versión 5 se incluye la actualización de todos los componentes compartidos (consulte la [Tabla 1-7 en la página 49](#)) y de todos los componentes de productos locales de los que dependa Access Manager.

Las dependencias de Access Manager deben actualizarse en el siguiente orden antes de actualizar Access Manager. Puede omitir todas aquellas dependencias que ya se hayan actualizado.

1. **Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#). Sin embargo, el programa de instalación actualizará automáticamente los componentes compartidos de Java ES cuando realice una instalación nueva de la Versión 5 de Access Manager.
2. **Directory Server.** Directory Server pocas veces reside en el mismo equipo que Access Manager. Sin embargo, las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en [“Actualización de Directory Server desde Java ES Versión 2” en la página 123](#).
3. **Software de contenedor web.** Las instrucciones para actualizar Web Server o Application Server están disponibles en [“Actualización de Web Server desde Java ES Versión 3” en la página 168](#) y en [“Actualización de Application Server desde Java ES Versión 2” en la página 235](#), respectivamente.

Actualice el esquema de directorio

Si se ha configurado Directory Server con la Herramienta de preparación de directorios de Sun Java Communications Suite (`comm_dssetup.pl`) para admitir componentes de Communication Suite como, por ejemplo, Messaging Server y Calendar Server, se debe actualizar en primer lugar el esquema de directorio utilizando la Herramienta de preparación de directorios de la versión 6.4 *antes de* actualizar Access Manager (consulte la *Sun Java Communications Suite 5 Upgrade Guide*, <http://docs.sun.com/doc/819-7561>). Realice esta tarea previa a la actualización después de actualizar las dependencias de Access Manager.

Vuelva a indexar el directorio

Para evitar complicaciones al realizar la actualización de Access Manager, después de haber actualizado el esquema de directorio (consulte más arriba [“Actualice el esquema de directorio,”](#)), tendrá que volver a indexar manualmente el sufijo raíz del directorio de Access Manager como se indica a continuación:

Versión 2-Versión 4 de Directory Server:

1. `cd serverRoot/slapd-`hostname``
2. `./db2index.pl -D "cn=directory manager" -w passwordFile -n databaseName`

donde la variable de nombre de base de datos, *databaseName*, es por defecto `userRoot`.

Versión 5 de Directory Server:

1. `cd DirServer-base/ds6/bin`
2. `./dsconf reindex -D "cn=Directory Manager" -e -w passwordFile suffix`
 donde
 - e significa conexión no segura
 - D es el administrador de directorios
 - w es un archivo de contraseñas que sólo contiene la contraseña
 - suffix* (sufijo) es el Access Manager sufijo raíz del directorio.

Dependiendo del número de entradas del directorio, puede llevar bastante tiempo completar la reindexación.

Actualización de la Versión 2 de Access Manager

El procedimiento de actualización de Access Manager de la Versión 2 a la 5 depende del contenedor web en el que se implemente el software de Access Manager.

Actualización de la Versión 2 de Access Manager: contenedor web Web Server

Para actualizar Access Manager a la Versión 5, al implementarlo en el contenedor web Web Server, siga las instrucciones que aparecen en [“Actualización de la Versión 4 de Access Manager” en la página 295](#) y sustituya toda referencia a la Versión 4 por la Versión 2.

Actualización de la Versión 2 de Access Manager: contenedor web Application Server

Existen dos formas de actualizar Access Manager de la Versión 2 a la Versión 5 cuando se ha implementado en el contenedor web de Application Server:

- **Se ha realizado una nueva instalación de la Versión 5 de Application Server.**
 En ese caso, para actualizar Access Manager de la Versión 2 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de la Versión 4 de Access Manager” en la página 295](#) y sustituya toda referencia a la Versión 4 por la Versión 2.

- **Se ha actualizado Application Server de la Versión 2 a la Versión 5.** En este caso, la instancia de la Versión 2 de Application Server en la que se implementó originalmente Access Manager (*instanceName*), cuando se actualizó a la Versión 5, se migró a un agente del nodo creado por el proceso de actualización. Para actualizar Access Manager en esta instancia actualizada de Application Server es necesario llevar a cabo los siguientes pasos:

Resumen de la actualización

El proceso de actualización de Access Manager consta de los siguientes pasos:

1. [Actualización del software de acceso móvil de Access Manager.](#)
2. [Elimine la versión de Access Manager de Java ES Versión 2.](#) Utilice la secuencia de comandos `ampre71upgrade` .
3. [Si la actualización a la Versión 5 tiene que adaptarse a la configuración regional, elimine los paquetes traducidos de la Versión 2.](#) Este paso tiene que llevarse a cabo manualmente.
4. [Instale la versión de Access Manager de Java ES Versión 5.](#) Utilice el programa de instalación de Java ES con la opción Configurar más tarde.
5. [Vuelva a personalizar los archivos JSP para Access Manager.](#)
6. [Asegúrese de que Directory Server se esté ejecutando.](#)
7. [Inicie las siguientes instancias de Application Server:](#) Domain Administration Server (DAS), agente del nodo e instancia del servidor en los que se haya implementado Access Manager.
8. [Anule la implementación de Access Manager y vuelva a configurar e implementar la instancia en Application Server.](#) Utilice la secuencia de comandos `amconfig`.
9. [Verifique que la información de Access Manager `classpath-suffix` y `server-classpath` se ha migrado al archivo de la Versión 5 de Application Server `domain.xml`.](#)
10. [Detenga Domain Administration Server \(DAS\), el nodo del agente y la instancia del servidor.](#)
11. [Reinicie DAS, el nodo del agente y la instancia del servidor.](#)
12. [Actualice la estructura y el esquema de directorio.](#) Utilice la secuencia de comandos `amupgrade`.

Estos pasos se describen en el siguiente procedimiento.

Procedimiento de actualización

1. Actualización del software de acceso móvil de Access Manager.

El software de acceso móvil de Access Manager debe actualizarse mediante la aplicación de revisiones en la Versión 2. Las revisiones necesarias se muestran en la siguiente tabla:

Tabla 14-13 Revisiones ¹ para la actualización del software de acceso móvil de Access Manager

Descripción	Id. de revisión: Solaris 9 y 10	Id. de revisión: Linux
Software de Mobile Access	119530-05 (SPARC)	119532-05
	119531-05 (x86)	• sun-identity-mobileaccess-6.2-25.3.i386.rpm • sun-identity-mobileaccess-config-6.2-25.3.i386.rpm

1. Los números de revisiones suponen la revisión mínima necesaria para actualizar a Java ES Versión 5. Si aparecen nuevas revisiones, utilícelas en lugar de las que aparecen en la tabla.

- a. Obtenga las revisiones necesarias mediante los números de revisión que aparecen en la [Tabla 14-6](#).

Las revisiones pueden descargarse en /tmp desde:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

- b. Lleve a cabo cualquiera de los procedimientos previos a la revisión indicados en los archivos de revisión README.
- c. Obtenga los valores de los siguientes parámetros que le solicitará la revisión:

Tabla 14-14 Parámetros de revisión de Mobile Access

Parámetro	Valor
DN de administrador de directorios	valor predeterminado: cn=Directory Manager
Contraseña de administrador de directorios	

- d. Aplique las revisiones que aparecen en la [Tabla 14-6](#).

```
En Solaris:
patchadd patch_ID

En Linux:
./update
```

Lleve a cabo cualquiera de los procedimientos posteriores a la revisión indicados en los archivos de revisión README.

- 2. Elimine la versión de Access Manager de Java ES Versión 2.
 - a. Inicie sesión como root en el equipo en el que resida la Versión 4 de Access Manager o conviértase en superusuario.

su -
 - b. Cambie el directorio al directorio *os_arch/Product/identity_svr/Tools* en la distribución de Java ES Versión 5, donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.
 - c. Obtenga los valores de los siguientes parámetros que le solicitará la secuencia de comandos *ampre71upgrade* :

Tabla 14-15 Parámetros de configuración de Access Manager *ampre71upgrade*

Parámetro	Valor
Host de Directory Server	Defina el nombre completo: <i>hostname.domain</i>
Puerto de Directory Server	Especifique un número de puerto que no sea SSL ¹ Valor predeterminado: 389
DN de administrador de nivel superior	Valor predeterminado: <i>uid=amadmin,ou=People,default_org_DN</i>
Contraseña del administrador de nivel superior:	
Directorio de almacenamiento de las copias de seguridad de los archivos	Valor predeterminado: <i>AccessManager-base</i>

1. Debe especificar un puerto SSL de Directory Server diferente del valor SSL predeterminado, 636.

- d. Asegúrese de que Directory Server se esté ejecutando. De lo contrario, inícielo.

- e. Ejecute la secuencia de comandos `ampre71upgrade`.

```
./ampre71upgrade
```

La secuencia de comandos realiza una copia de seguridad de los archivos de configuración de Access Manager y elimina los paquetes de la Versión 4 básica (los paquetes traducidos deben eliminarse manualmente según lo indicado en el [Paso 3](#)).

3. Si la actualización a la Versión 5 tiene que adaptarse a la configuración regional, elimine los paquetes traducidos de la Versión 2.

La secuencia de comandos `ampre71upgrade` ejecutada anteriormente en el [Paso 2](#) no elimina los paquetes traducidos, por lo que tendrá que eliminarlos manualmente como se indica a continuación.

En Solaris:

- a. Busque los paquetes traducidos.

```
pkginfo | grep SUNWaml
pkginfo | grep SUNWamclnt
pkginfo | grep SUNWamdistauth
```

- b. Elimine cualquier paquete traducido que haya encontrado en el [Paso a](#) mencionado anteriormente.

```
pkgrm SUNWamlLocale
pkgrm SUNWamlLocale
pkgrm SUNWamdistauthLocale
```

En Linux:

- a. Busque los RPM traducidos.

```
rpm -qa | grep sun-identity-sdk-*
rpm -qa | grep sun-identity-clientsdk-*
rpm -qa | grep sun-identity-distauth-*
```

- b. Elimine cualquier RPM traducido que haya encontrado en el [Paso a](#) mencionado anteriormente.

```
rpm -e sun-identity-sdk-Locale-*
rpm -e sun-identity-clientsdk-Locale-*
rpm -e sun-identity-distauth-Locale-*
```

4. Instale la versión de Access Manager de Java ES Versión 5.

Lleve a cabo estos pasos:

- a. Inicie el programa de instalación de Java ES en el equipo que aloje la Versión 2 de Access Manager.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*. (Utilice la opción *installer -nodisplay* para la interfaz de línea de comandos).

Una vez mostradas las páginas de bienvenida y acuerdo de licencia, aparecerá la página de selección de componentes. (Cuando se detectan componentes instalados que pueden ser actualizados directamente con el programa de instalación de Java ES, éstos aparecen con el estado “actualizables”).

- b. Seleccione Access Manager en la página de selección de componentes.
 - c. Especifique el mismo directorio de instalación en el que se haya instalado la Versión 2.
 - d. Seleccione la opción Configurar más tarde.
 - e. Si fuera necesario, seleccione la opción para instalar paquetes traducidos.
 - f. Una vez completada la instalación, salga del programa de instalación de Java ES.
5. Vuelva a personalizar los archivos JSP para Access Manager.

Vuelva a aplicar las personalizaciones de la Versión 2 a los archivos JSP de la consola de Access Manager y a la interfaz de usuario de autenticación (IU) que guardó en “Copia de seguridad de los archivos personalizados del contenedor web” en la página 294.

A continuación, copie los archivos JSP personalizados en los directorios correspondientes:

- Consola de Access Manager que sólo admite el modo tradicional
AccessManager-base/web-src/applications/console
- IU de autenticación:
AccessManager-base/web-src/services/config/auth/default o
AccessManager-base/web-src/services/config/auth/default_Locale
(donde *Locale* es un indicador de configuración regional como, por ejemplo, *ja*)

Para obtener más información, consulte la *Sun Java System Access Manager 7.1 Developer's Guide*, <http://docs.sun.com/doc/819-4675>.

6. Asegúrese de que Directory Server se esté ejecutando.
7. Inicie las siguientes instancias de Application Server:

En los siguientes comandos, y en los pasos siguientes, se utilizan las convenciones que aparecen a continuación:

- *nodeagentName* tiene el formato *hostName_domainName*, pero su variable predeterminada es simplemente *hostName*
- La variable de nombre de dominio, *domainName*, predeterminada es *domain1*.
- La variable de nombre de instancia, *instanceName*, predeterminada es *server1*

NOTA Asegúrese de iniciar de forma independiente el agente del nodo mediante la opción `startinstances=false` antes de iniciar la instancia del servidor, como se indica a continuación.

- a. Inicie Domain Administration Server (DAS).

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

- b. Inicie el agente del nodo al que se ha migrado la instancia actualizada de Application Server:

```
AppServer8-base/bin/asadmin start-node-agent
--startinstances=false --user admin_ID nodeagentName
```

- c. Inicie la instancia del servidor en la que se ha implementado Access Manager (*instanceName*), si aún no se está ejecutando esa instancia del servidor.

```
AppServer8-base/bin/asadmin start-instance --user admin_ID
instanceName
```

8. Anule la implementación de Access Manager y vuelva a configurar e implementar la instancia en Application Server.

- a. Si el contenedor web se está ejecutando en modo SSL, asegúrese de que los certificados SSL del contenedor no hayan caducado y sigan siendo válidos.

- b. Cree un archivo de entrada `amconfig` basado en el archivo de entrada de plantilla `amsamplesilent`:

```
cp amsamplesilent config-file
```

(En los pasos siguientes, *config-file* se supone que reside en el mismo directorio que `amsamplesilent`.)

- c. Establezca los parámetros de configuración en *config-file*.

Todos los parámetros deben establecerse correctamente. Algunos de los valores pueden migrarse desde el archivo `AMConfig.properties`, aunque otros son más específicos del proceso de actualización, como se muestra en la siguiente tabla.

Tabla 14-16 Parámetros de configuración de Access Manager `amconfig`

Parámetro	Valor
Parámetros de actualización	
DEPLOY_LEVEL	Establézcalo en 26 (para la anulación de la implementación) ó en 1 (para la reconfiguración e implementación)
DIRECTORY_MODE	Establézcalo en 5
AM_REALM ¹	Establézcalo en disabled (si el modo tradicional está habilitado) Establézcalo en enabled (si el modo de dominio está habilitado) Valor predeterminado: enabled
JAVA_HOME	Establézcalo en el directorio de JDK de la Versión 5: /usr/java/jdk1.5.0_04/
WEB_CONTAINER	Establézcalo en AS8 para Application Server 8.x y rellene solamente la sección correspondiente de <i>config-file</i> .
AS81_INSTANCE (Si se utiliza Application Server 8.x actualizado desde Application Server 7.x como contenedor web)	Establézcalo en Application Server 7.x <i>instanceName</i> , cuyo valor predeterminado es <code>server1</code>
AS81_INSTANCE_DIR (Si se utiliza Application Server 8.x como contenedor web)	Establézcalo en el directorio de dominio de Application Server 8.x para la instancia, cuyo valor predeterminado es <i>AppServer8Config-base/domains/domain1</i>

Tabla 14-16 Parámetros de configuración de Access Manager `amconfig`

Parámetro	Valor
AS81_DOCS_DIR (Si se utiliza Application Server 8.x como contenedor web)	Establezca el valor en el directorio de dominio deApplication Server 8.x para la instancia, cuyo valor predeterminado es <i>AppServer8Config-base/domains/domain1/docroot</i>
Migrados desde <code>AMConfig.properties</code>	
SERVER_PROTOCOL	<code>com.iplanet.am.server.protocol</code>
SERVER_PORT	<code>com.iplanet.am.server.port</code>
SERVER_HOST	<code>com.iplanet.am.server.host</code>
DS_HOST	<code>com.iplanet.am.directory.host</code>
DS_PORT	<code>com.iplanet.am.directory.port</code>
ROOT_SUFFIX ²	<code>com.iplanet.am.defaultOrg</code>
CONSOLE_DEPLOY_URI	<code>com.iplanet.am.console.deploymentDescriptor</code>
SERVER_DEPLOY_URI	<code>com.iplanet.am.services.deploymentDescriptor</code>
PASSWORD_DEPLOY_URI	<code>com.sun.identity.password.deploymentDescriptor</code>
AM_ENC_PWD ²	<code>am.encryption.pwd³</code>

- 1. Para más información sobre el modo tradicional y el de dominio, consulte [“Problemas de compatibilidad” en la página 286](#).
- 2. El valor de este parámetro tiene que ser el mismo que el de la versión anterior de Access Manager.
- 3. Cuando se implementan Access Manager y Access Manager SDK, el valor de esta propiedad debe ser el mismo para la instancia de Access Manager y su instancia asociada de Access Manager SDK.

Para los demás parámetros, especifique los mismos valores utilizados en la configuración de la Versión 2 que está actualizando, a menos que cambie el contenedor web o las contraseñas.

- d. Ejecute `amconfig` para anular la implementación de Access Manager
Establezca el valor de `DEPLOY_LEVEL` de `config-file` en 26.

```
cd /AccessManager-base/bin
./amconfig -s AccessManager-base/bin/config-file
```

- e. Compruebe que se está ejecutando el contenedor de agentes común.

```
netstat -an | grep 11163
```

Si no se está ejecutando, inícielo.

```
/usr/sbin/cacoadm start
```

- f. Ejecute `amconfig` para volver a configurar Access Manager e implementarlo en un contenedor web.

Establezca el valor de `DEPLOY_LEVEL` de *config-file* en 1.

```
cd /AccessManager-base/bin
./amconfig -s AccessManager-base/bin/config-file
```

9. Verifique que la información de Access Manager `classpath-suffix` y `server-classpath` se ha migrado al archivo de la Versión 5 de Application Server `domain.xml`.

- a. Copie la información de `classpath-suffix` y `server-classpath` de Access Manager, ubicada en el archivo `server.xml` de la instancia de Application Server de la Versión 2 en la que se implementó originalmente Access Manager:

```
AppServer7Config-base/domains/domainName/instanceName/config/server.xml
```

- b. Asegúrese de que las entradas de `classpath-suffix` y `server-classpath` se han anexado al archivo `domain.xml` de la instancia actualizada Application Server en la que se ha implementado Access Manager:

```
AppServer8Config-base/nodeagents/nodeagentName/instanceName/
config/domain.xml
```

La información de la ruta de clase debería agregarse al bloque `instanceName-config` del archivo `domain.xml` de Application Server de la Versión 5. Este bloque comienza con la siguiente línea:

```
<config dynamic-reconfiguration-enabled="true"
name="instanceName-config">
```

10. Actualice la estructura y el esquema de directorio.

La Versión 5 de Access Manager coexiste con la estructura de directorio de la Versión 4, aunque ésta deba modificarse para que pueda admitir las funciones de la Versión 5. Actualice la estructura y el esquema de directorio de Access Manager a la Versión 5 ejecutando la secuencia de comandos `amupgrade`, que está instalada en el siguiente directorio:

- o En Solaris:
`AccessManager-base/upgrade/scripts`
- o En Linux:
`AccessManager_base/identity/upgrade/scripts`
- a. Obtenga los valores de los siguientes parámetros que le solicitará la secuencia de comandos `amupgrade` :

Tabla 14-17 Parámetros de configuración de Access Manager amupgrade

Parámetro	Valor
Host de Directory Server	Defina el nombre completo: <i>nombrehost.dominio</i>
Puerto de Directory Server	Especifique un número de puerto que no sea SSL ¹ Valor predeterminado: 389
DN de administrador de directorios	Valor predeterminado: cn=Directory Manager
Contraseña del administrador de directorios	
DN de administrador de nivel superior	Valor predeterminado: uid=amadmin,ou=People,default_org_DN
Contraseña del administrador de nivel superior:	
Habilitar modo de dominio (Este valor de parámetro no se solicita cuando se actualiza desde la Versión 4 en modo de dominio).	Y/N: Yes (Sí) implica la activación del modo de dominio y la migración de los servicios de datos al nuevo árbol de dominio. No (valor predeterminado) implica que los servicios de datos permanecen en el modo tradicional.

1. El proceso de actualización no se completará satisfactoriamente si especifica un puerto SSL de Directory Server como, por ejemplo, el valor SSL predeterminado, 636.

b. Ejecute la secuencia de comandos amupgrade.

```
cd AccessManager-base/upgrade/scripts
./amupgrade
```

Si la actualización se realiza con éxito, la secuencia de comandos muestra “Upgrade completed.”

c. Consulte el siguiente archivo de registro de actualización para obtener información sobre las extensiones del esquema de directorio:

```
En Solaris:
/var/sadm/install/logs/
    Sun_Java_System_Access_Manager_upgrade_dit_log.mmddhhmm

En Linux:
/var/log/Sun_Java_System_Access_Manager_upgrade_dit_log.mmddhhmm
```

11. Detenga Domain Administration Server (DAS), el nodo del agente y la instancia del servidor.

Estas instancias se iniciaron en el [Paso 7 en la página 329](#).

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
domainName
```

```
AppServer8-base/bin/asadmin stop-node-agent --user admin_ID
nodeagentName
```

12. Reinicie DAS, el nodo del agente y la instancia del servidor.

NOTA Asegúrese de iniciar de forma independiente el agente del nodo mediante la opción `startinstances=false` antes de iniciar la instancia del servidor, como se indica a continuación.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

```
AppServer8-base/bin/asadmin start-node-agent --port DASportNumber
--startinstances=false --user admin_ID --password password
nodeagentName
```

```
AppServer8-base/bin/asadmin start-instance --port DASportNumber
--user admin_ID --password password instanceName
```

El valor predeterminado de *DASportNumber* es 4848.

Verificación de la actualización de Access Manager

Una vez completado el proceso de actualización, compruebe que se haya realizado con éxito como se describe en [“Verificación de la actualización de Access Manager” en la página 306](#).

Tareas posteriores a la actualización

Si está utilizando el servicio Security Assertion Markup Language (SAML), deberá agregar y habilitar el módulo de autenticación SAML utilizando la consola de Access Manager. Para obtener información sobre cómo crear una instancia del módulo de autenticación SAML, consulte la *Sun Java System Access Manager Administration 7.1 Guide* (<http://docs.sun.com/doc/819-4670>).

Anulación de la actualización

No se proporciona ninguna secuencia de comandos para restablecer Access Manager al estado anterior a la actualización. Este proceso debe realizarse manualmente utilizando los datos de Access Manager de los que se realizó una copia de seguridad como parte de las tareas previas a la actualización (consulte [“Copia de seguridad de los archivos de depuración y registro de Access Manager de la Versión 4” en la página 294](#)). El procedimiento para deshacer la actualización es poco práctico debido a su complejidad.

Actualización de varias instancias

En algunas arquitecturas de implementación, Access Manager se implementa en varios sistemas informáticos para proporcionar alta disponibilidad y escalabilidad.

A menudo es recomendable actualizar las instancias de Access Manager secuencialmente sin necesidad de interrumpir el servicio. El procedimiento que se sigue para llevar a cabo una actualización de Access Manager de la Versión 2 a la Versión 5 está basado en la siguiente restricción: La Versión 5 de Access Manager *no* puede coexistir con la estructura de directorio de la Versión 2. Sin embargo, si se replican las instancias de Directory Server, como se muestra en la [Figura 14-2](#), entonces puede realizar una actualización por turnos como se indica en [“Actualización de varias instancias” en la página 315](#).

Portal Server

En este capítulo se describe cómo actualizar Portal Server a Java ES 5 (Versión 5): Sun Java System Portal Server 7.1.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Portal Server” en la página 339
- “Actualización de Portal Server desde Java ES Versión 4” en la página 346
- “Actualización de Portal Server desde Java ES Versión 3” en la página 377
- “Actualización de Portal Server desde Java ES Versión 2” en la página 380
- “Actualización de Portal Server desde la Versión intermedia 7.0” en la página 391

NOTA Las ubicaciones de los archivos de este capítulo se especifican en relación con las rutas de directorios a las que se denomina *PortalServer6-base* y *PortalServer6Config-base* (Portal Server 6.x) y *PortalServer7-base* y *PortalServer7Config-base* (Portal Server 7.x). Debe haberse especificado, al menos, parte de estas rutas como directorio de instalación durante la instalación inicial de Portal Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado.

Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.

Tabla 15-1 Portal Server Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>PortalServer6-base</i>	/opt/SUNWps	/opt/sun/portal
<i>PortalServer6Config-base</i>	/etc/opt/SUNWps	/etc/opt/sun/portal
<i>PortalServer7-base</i>	/opt/SUNWportal	/opt/sun/portal
<i>PortalServer7Config-base</i>	/etc/opt/SUNWportal	/etc/opt/sun/portal
<i>PortalServer7Data-base</i>	/var/opt/SUNWportal	/var/opt/sun/portal

Visión general de la actualización de Portal Server

En esta sección se describen los siguientes aspectos generales de Portal Server que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Portal Server de Java ES Versión 5](#)
- [Guía de actualización de Portal Server](#)
- [Datos de Portal Server](#)
- [Estrategia de actualización para Portal Server](#)

Acerca de Portal Server de Java ES Versión 5

El componente Portal Server de Java ES Versión 5 representa un avance importante en relación con la Versión 4, ya que incluye una serie de nuevas mejoras y funciones. Gran parte de estos cambios se realizaron en una Versión intermedia (IFR, Interim Feature Release) posterior a la Versión 4. La Versión 5 sólo presenta ligeros cambios en las funciones en relación con la versión IFR. Para obtener información sobre las mejoras y las nuevas funciones de la versión IFR, consulte *Sun Java System Portal Server 7.1 Release Notes*, <http://docs.sun.com/doc/819-4986/6n4l3f365?a=view>. En concreto, se ha sustituido la interfaz administrativa de línea de comandos de la Versión 4 por el comando `psadmin`.

Guía de actualización de Portal Server

La [Tabla 15-2](#) muestra las rutas de actualización compatibles de Portal Server para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 15-2 Rutas de actualización a Java ES 5 (Versión 5): Portal Server 7.1

Versión de Java ES			
Java ES	Portal Server Versión	Enfoque general	Reconfiguración necesaria
Versión intermedia (IFR)	Sun Java System Portal Server IFR 7.0 2005Q4	Actualización directa: Se realiza mediante la aplicación de revisiones y, a continuación, el uso de una secuencia de comandos de actualización.	Las personalizaciones deben aplicarse de nuevo manualmente.
Versión 4	Sun Java System Portal Server 6.3.1 2005Q4	Actualización directa: Se realiza mediante una secuencia de comandos de actualización.	Las personalizaciones deben aplicarse de nuevo manualmente.
Versión 3	Sun Java System Portal Server 6.3.1 2005Q1	Actualización directa: Se realiza mediante una secuencia de comandos de actualización.	Las personalizaciones deben aplicarse de nuevo manualmente.
Versión 2	Sun Java System Portal Server 6.3 2004Q2	Actualización directa: Se realiza mediante una secuencia de comandos de actualización.	Las personalizaciones deben aplicarse de nuevo manualmente.
Versión 1	Sun ONE Portal Server 6.2 (2003Q4)	Sin actualización directa: Aunque puede realizarse actualizando primero a la Versión 3 y, a continuación, de la Versión 3 a la Versión 5.	Datos de configuración
Versiones anteriores de Java ES		Sin actualización directa.	

Datos de Portal Server

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Portal Server.

Tabla 15-3 Portal Server Uso de datos

Tipo de datos	Ubicación	Uso
Datos de configuración	<i>PortalServer6Config-base/</i>	Configuración de Portal Server.

Tabla 15-3 Portal Server Uso de datos (*continúa*)

Tipo de datos	Ubicación	Uso
Archivos de configuración y control de acceso al contenedor web	Web Server 7.0 (Java ES Versión 5)Archivos <code>server.policy</code> y <code>server.xml</code> en <code>WebServer7Config-base/https-configName/config</code>	Configuración de la instancia del contenedor web de Portal Server
	Web Server 6.x (Java ES Versión 2, 3 y 4)Archivos <code>server.policy</code> y <code>server.xml</code> en <code>WebServer6-base/https-hostname/config</code>	
	Application Server 8.x (Java ES Versión 3, 4 y 5):Archivos <code>server.policy</code> y <code>domain.xml</code> en <code>AppServer8Config-base/domains/domainName/config</code>	
	Application Server 7.x (Java ES Versión 2):Archivos <code>server.policy</code> y <code>server.xml</code> en <code>AppServer7Config-base/domains/domainName/config</code>	
Datos de personalización	<code>PortalServer6Config-base/desktop</code>	Archivos JAR para módulos personalizados Escritorio de ejemplo personalizado de Portal Server
Esquema de directorio	Directory Server	Portal Server depende de las configuraciones de los servicios, como Portal Desktop, y de los datos de perfil del usuario almacenados en un directorio.
Configuración de servicios		
Datos de usuario		
Datos de aplicación dinámicos	Ninguna	Portal Server no almacena de forma persistente datos de aplicación como, por ejemplo, el estado de la sesión.

Estrategia de actualización para Portal Server

La estrategia utilizada para la actualización de Portal Server depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Portal Server presentando una serie de problemas que pueden influir en el plan de actualización de Portal Server.

Problemas de compatibilidad

La Versión 5 de Portal Server presenta cambios para la interfaz pública en el comando `psadmin` utilizado para administrar los componentes de Portal Server y Portal Server Secure Remote Access. Consulte *Sun Java System Portal Server 7.1 Command-Line Reference*, <http://docs.sun.com/doc/819-5030>.

Por lo tanto, la Versión 5 de Portal Server no es compatible con las versiones anteriores ni con las versiones anteriores de los componentes de Portal Server Secure Remote Access (incluidos la puerta de enlace de SRA, proxy Rewriter y proxy Netlet), excepto durante el periodo de transición en el que se realiza la actualización por turnos de las implementaciones de varias instancias. Todas las instancias de Portal Server deben sincronizarse, junto con las instancias de los componentes de Portal Server Secure Remote Access, en Java ES Versión 5.

Además, los componentes individuales de Portal Server, incluido el componente de acceso móvil, no son compatibles con las versiones anteriores; todos deben sincronizarse a Java ES Versión 5.

Además, existe una incompatibilidad entre las estructuras de datos de Directory Server utilizadas por la Versión 5 de Portal Server y las versiones anteriores de Portal Server. Esta incompatibilidad afecta a la actualización por turnos de varias instancias de Portal Server que utilicen los mismos datos de Directory Server.

Portal Server Dependencias

Las dependencias de Portal Server con respecto a otros componentes de Java ES pueden afectar al procedimiento de actualización y reconfiguración del software de Portal Server. Por ejemplo, los cambios en las interfaces o las funciones de Portal Server pueden requerir las versiones actualizadas de los componentes de los que depende Portal Server. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Portal Server presenta relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Portal Server presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Contenedor web.** Portal Server presenta una relación de dependencia obligatoria con respecto a los servicios de contenedor web proporcionados por Java ES Web Server o Java ES Application Server, o los contenedores de terceros de Weblogic y WebSphere.

NOTA No se admite la actualización de Portal Server a la Versión 5 para las implementaciones realizadas en contenedores web de terceros. Para las implementaciones efectuadas en contenedores web de Weblogic y WebSphere, debe realizar una nueva instalación de la Versión 5 de Portal Server.

- **Access Manager (o Access Manager SDK).** Portal Server presenta una relación de dependencia obligatoria con Access Manager para proporcionar servicios de autenticación y autorización para usuarios finales, incluido el inicio de sesión único. Si Access Manager se ejecuta en un equipo remoto, Access Manager SDK debe estar disponible de forma local.
- **Directory Server.** Portal Server presenta una relación de dependencia obligatoria con Directory Server, que almacena los datos del usuario a través de Access Manager. Por lo tanto, es posible que las actualizaciones de Portal Server necesiten las extensiones del esquema de directorio.
- **Portal Server Secure Remote Access.** Portal Server presenta una relación de dependencia opcional con Portal Server Secure Remote Access, que proporciona acceso remoto seguro mediante los componentes de puerta de enlace, proxy Rewriter y proxy Netlet.
- **Java DB.** Portal Server presenta una relación de dependencia opcional con Java DB, que proporciona compatibilidad con varias aplicaciones de portlet.
- **Service Registry.** Portal Server presenta una relación de dependencia obligatoria con Service Registry, que proporciona las bibliotecas necesarias para la compilación.
- **Communications Express.** Portal Server presenta una relación de dependencia opcional con Communications Express, un componente de Sun Java Communications Suite que se utiliza para proporcionar canales de calendario y mensajería a los usuarios finales. Communications Express ya no es un componente de producto de Java ES.

Problemas de la actualización selectiva

Aunque Java ES Versión 5 admite generalmente la actualización selectiva de todos los componentes en un equipo, el hecho de que Portal Server presente relaciones de dependencia con muchos otros componentes de Java ES dificulta en gran medida la posibilidad de certificar combinaciones arbitrarias de los componentes entre diversas versiones comerciales de Java ES.

Por este motivo, Portal Server admite un conjunto restringido de escenarios de actualización en relación con Access Manager y los contenedores web.

- **Si va a actualizar Portal Server desde Java ES Versión 4.** Puede actualizar Directory Server, Access Manager y el contenedor web (Web Server o Application Server) a la Versión 5 antes de actualizar Portal Server o puede actualizar *sólo* Portal Server a la Versión 5 (dejando el resto de componentes en el nivel de la Versión 4), aunque no puede dejar algunas dependencias en la Versión 4 y actualizar otras a la Versión 5.
- **Si va a actualizar Portal Server desde Java ES Versión 3.** Debe actualizar Directory Server, Access Manager y el contenedor web (Web Server o Application Server) a la Versión 4 o 5 antes de actualizar Portal Server, aunque no puede dejar ninguna dependencia en la Versión 3 ni actualizar algunas a la Versión 4 y otras a la Versión 5.
- **Si va a actualizar Portal Server desde Java ES Versión 2.** Debe actualizar Directory Server, Access Manager y el contenedor web (Web Server o Application Server) a la Versión 4 o 5 antes de actualizar Portal Server, aunque no puede dejar ninguna dependencia en la Versión 2 ni actualizar algunas a la Versión 4 y otras a la Versión 5.

Escenarios de actualización del contenedor web

Portal Server puede implementarse en un contenedor web proporcionado por Web Server o Application Server. Por lo tanto, la actualización de Portal Server a la Versión 5 puede complicarse debido a la posibilidad de tener que actualizar también a la Versión 5 el contenedor web en el que se ha implementado. En este sentido, hay una serie de escenarios posibles de actualización del contenedor web, que se enumeran en la siguiente tabla.

Tabla 15-4 Escenarios de actualización del contenedor web para la actualización de Portal Server

Escenario	Contenedor web en el que se ha implementado originalmente Portal Server	Contenedor web en el que se ha implementado Portal Server después de la actualización	Rutas de actualización pertinentes de Portal Server: actualización desde
Escenario 1	Web Server 6.x	Web Server 6.x	Versión 2 Versión 3 Versión 4 IFR 7.0

Tabla 15-4 Escenarios de actualización del contenedor web para la actualización de Portal Server

Escenario	Contenedor web en el que se ha implementado originalmente Portal Server	Contenedor web en el que se ha implementado Portal Server después de la actualización	Rutas de actualización pertinentes de Portal Server: actualización desde
Escenario 2	Web Server 6.x	Web Server 7.0	Versión 2 Versión 3 Versión 4 IFR 7.0
Escenario 3	Application Server 8.1	Application Server 8.1	Versión 3 Versión 4 IFR 7.0
Escenario 4	Application Server 8.1	Application Server 8.2	Versión 3 Versión 4 IFR 7.0
Escenario 5	Application Server 7.x	Application Server 8.2	Versión 2

Al realizar la actualización de Portal Server (por ejemplo, al utilizar la secuencia de comandos psupgrade), debe asegurarse de proporcionar los valores adecuados al escenario de actualización de la [Tabla 15-4](#) que se aplique, sobre todo cuando se realice una actualización importante de la versión del contenedor web.

Actualización de Portal Server desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Portal Server desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5).

NOTA	Esta sección no aborda la siguiente situación especial: Portal Server se ha implementado un contenedor web Application Server y se ha actualizado de la Versión 2 a la Versión 3 o 4 antes de efectuar la actualización a la Versión 5. La ruta de actualización mencionada anteriormente no se permite en la actualidad.
-------------	---

En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Portal Server](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Portal Server de Java ES de la Versión 4 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque de actualización general.** La actualización se realiza mediante una secuencia de comandos de actualización, `psupgrade`. La secuencia de comandos instala los nuevos paquetes, migra los datos de configuración, si es necesario, actualiza los archivos de traducción y vuelve a implementar las aplicaciones web de Portal Server en el contenedor web.
- **Dependencias de actualización.** Portal Server presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Aunque la Versión 5 de Portal Server es compatible con la Versión 4 de estos componentes compartidos, es necesario actualizarlos debido a que la secuencia de comandos `psupgrade` utilizada para actualizar Portal Server requiere la Versión 5 del componente compartido ANT.

La Versión 5 de Portal Server presenta también relaciones de dependencia con un contenedor web, Access Manager y Directory Server, como se describe en [“Portal Server Dependencias” en la página 342](#). Se admiten dos enfoques para actualizar estas dependencias (consulte [“Problemas de la actualización selectiva” en la página 343](#)):

- Los componentes de la Versión 4 satisfacen todas las dependencias (no se actualiza *ningún* componente a la Versión 5).
- Los componentes de la Versión 5 satisfacen todas las dependencias (se actualizan *todos* los componentes a la Versión 5).
- **Compatibilidad con versiones anteriores.** La Versión 5 de Portal Server no es compatible con la Versión 4.
- **Anulación de la actualización.** Para anular la actualización de la Versión 4 a la Versión 5 de Portal Server, se deben restablecer los paquetes y los datos del directorio de la Versión 4, además de volver a implementar las aplicaciones web de Portal Server en el contenedor web.
- **Problemas de plataforma.** El enfoque de actualización general de Portal Server es idéntico tanto en el sistema operativo Solaris como en Linux. Sin embargo, la Versión 5 de Portal Server se instala en una nueva ruta en el sistema operativo Solaris mientras que, en el sistema operativo Linux, se instala en la misma ruta que la Versión 4.

Actualización de la Versión 4 de Portal Server

En esta sección se describe cómo realizar una actualización de Portal Server de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización de la Versión 4](#)
- [Actualización de la Versión 4 de Portal Server \(Solaris\)](#)
- [Actualización de la Versión 4 de Portal Server \(Linux\)](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización de la Versión 4](#)
- [Deshacer la actualización \(Solaris\)](#)
- [Anulación de la actualización \(Linux\)](#)

Tareas previas a la actualización de la Versión 4

Antes de actualizar Portal Server, debe realizar las tareas siguientes:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Portal Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)
- [Copia de seguridad de la información de configuración de la Versión 4 de Portal Server](#)
- [Registre la configuración de la Máquina virtual de Java \(JVM\)](#)
- [Elimine la configuración del equilibrador de carga](#)
- [Elimine la configuración de Directory Proxy Server](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Portal Server, utilice el siguiente comando:

```
PortalServer6-base/bin/version
```

Tabla 15-5 Resultados de la verificación de la versión de Portal Server

Versión de Java ES	Número de versión de Portal Server
Versión 2	6.3
Versión 3	6.3.1
Versión 4	6.3.1 ¹
Versión IFR	7.0
Componente de producto de la	7.1

1. La única diferencia entre la Versión 3 y la 4 es una revisión. Puede buscar las revisiones de la Versión 4 mediante el comando `showrev -p | grep patch_ID` de Solaris y el comando `rpm -qa sun-portal-core` de Linux, y comparar las versiones con las que aparecen en la *Guía de actualización de Java ES Versión 4*.

Actualización de las dependencias de Portal Server

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5.

Aunque la Versión 5 de Portal Server es compatible con la Versión 4 de los componentes compartidos de Java ES, es necesario actualizar estos componentes debido a que la secuencia de comandos `psupgrade` utilizada para actualizar Portal Server requiere la Versión 5 del componente compartido ANT.

Si decide actualizar alguna de las dependencias de los componentes de productos de Portal Server a la Versión 5, deberán actualizarse *todas* (consulte [“Problemas de la actualización selectiva” en la página 343](#)). Las dependencias deben actualizarse en el orden siguiente (omitiendo aquéllas que es posible que ya se hayan actualizado) antes de actualizar Portal Server.

1. **Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69](#).
2. **Directory Server.** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [Capítulo 5, “Directory Server” en la página 107](#).
3. **Software de contenedor web.** Las instrucciones para actualizar Web Server o Application Server están disponibles en [Capítulo 7, “Web Server” en la página 141](#) y en [Capítulo 11, “Application Server” en la página 219](#), respectivamente.

NOTA

Al actualizar los contenedores web de terceros como, por ejemplo, los de Weblogic y WebSphere, puede interrumpirse Portal Server, ya que el proceso de actualización del contenedor sobrescribe las personalizaciones realizadas en estos contenedores para poder utilizar Portal Server.

En ese caso, debe volver a instalar y configurar Portal Server para los entornos de contenedor web actualizados.

4. **Access Manager (Access Manager SDK).** Las instrucciones para actualizar Access Manager a la Versión 5 están disponibles en el [Capítulo 14, “Access Manager” en la página 281](#).
5. **Portal Server Secure Remote Access.** Las instrucciones para actualizar Portal Server Secure Remote Access a la Versión 5 están disponibles en el [Capítulo 16, “Portal Server Secure Remote Access” en la página 411](#).
6. **Java DB.** Las instrucciones para actualizar Java DB a la Versión 5 están disponibles en el [Capítulo 8, “Java DB” en la página 171](#).
7. **Service Registry.** Las instrucciones para actualizar Service Registry a la Versión 5 están disponibles en el [Capítulo 12, “Service Registry” en la página 249](#).

- 8. Communications Express.** Las instrucciones para actualizar Communications Express a la Versión 5 están disponibles en la *Sun Java Communications Suite Upgrade Guide*, <http://docs.sun.com/doc/819-7561>.

Obtenga las contraseñas y la información de configuración necesarias

En función del escenario de actualización del contenedor web (consulte la [Tabla 15-4 en la página 344](#)), la secuencia de comandos `psupgrade` necesita que introduzca la información sobre las contraseñas y otros datos de configuración del contenedor web. La [Tabla 15-6](#) muestra la información necesaria para los diferentes escenarios de actualización del contenedor web. Asegúrese de recopilar la información pertinente antes de comenzar el proceso de actualización de Portal Server.

Tabla 15-6 Información necesaria para la secuencia de comandos `psupgrade` según el escenario de actualización del contenedor web

Información	Escenario de actualización n ³	Web Server 7.x Valores de ejemplo: Escenario 2	Application Server 8.x Valores de ejemplo: Escenario 5 ²
Actualización de Portal Server en Web Server 7.0 (sí/no)	2	Sí	N/D
Directorio de instalación del contenedor web	2 y 5	<i>WebServer7-base</i>	<i>AppServer8Install-base</i>
Nombre de la instancia del servidor virtual del contenedor web	2	<i>configName⁴</i>	N/D
Nombre de la instancia del contenedor web	5	N/D	server1
Directorio de la instancia del contenedor web	2	<i>WebServer7Config-base/https-configName³/</i>	N/D
Directorio de implementación de la instancia de Portal Server	5	N/D	<i>AppServer8Config-base/domains/domainName</i>
Puerto de la instancia del contenedor web	2 y 5	80	80
Protocolo de la instancia del contenedor web	2 y 5	http	http
Nombre de configuración del contenedor web	2	<i>configName³</i>	N/D
Nombre de dominio del contenedor web	5	N/D	domain1

Tabla 15-6 Información necesaria para la secuencia de comandos psupgrade según el escenario de actualización del contenedor web (*continúa*)

Información	Escenario de actualización ⁿ³	Web Server 7.x Valores de ejemplo: Escenario 2	Application Server 8.x Valores de ejemplo: Escenario 5 ²
Directorio raíz de documentos del contenedor web	2 y 5	WebServer7Config-base/ https-configName ³ /docs/	AppServer8Config-base/ domains/domainName/ docroot
Nombre del host de administración del contenedor web	2 y 5	localhost	localhost
Puerto de administración del contenedor Web	2 y 5	8989	4848
Protocolo de administración del contenedor web	2 y 5	https	https
Id. de usuario de administración del contenedor web	2 y 5	admin	admin
Contraseña de administración del contenedor web	De 2 a 5		
Contraseña maestra del contenedor web	De 3 a 5	N/D	
Contraseña del administrador de directorios (cn=Directory manager)	De 1 a 5		
Contraseña de usuario del registro de SRA ¹	De 1 a 5		
Contraseña de administración de Access Manager	De 1 a 5		
Contraseña de ldapuser de Directory Server	De 1 a 5		
Id. de instancia de Portal Server ²	De 1 a 5		

1. Esta información es necesaria para configurar los componentes de Portal Server Secure Remote Access cuando se instalan junto con Portal Server.

2. Debe especificarse un valor exclusivo que no sea nulo para este parámetro. Los valores deben ser alfanuméricos y pueden incluir un guión (-).

3. El escenario de actualización del contenedor web núm. 5 se aplica a la actualización de Portal Server desde la Versión 2.

4. El valor predeterminado de configName es hostName.domainName.

Copia de seguridad de la información de configuración de la Versión 4 de Portal Server

Al actualizar Portal Server a la Versión 5, no es necesario reconfigurar el software de Portal Server. Sin embargo, como medida de protección, la secuencia de comandos `psupgrade` realiza una copia de seguridad de los directorios en los que se almacena la información de configuración:

PortalServer6Config-base/

NOTA	Se recomienda realizar una copia de seguridad de la instancia de Directory Server en la que se almacenan los perfiles de usuarios y otros datos de Portal Server. Sin esos datos, no es posible anular la actualización a la Versión 5 de Portal Server.
-------------	--

Registre la configuración de la Máquina virtual de Java (JVM)

Antes de realizar la actualización de Portal Server, registre la siguiente configuración de JVM del contenedor web si es distinta de los valores predeterminados:

```
<jvm-options>-XX:MaxPermSize=256m</jvm-options>
<jvm-options>-XX:+CMSPermGenSweepingEnabled</jvm-options>
<jvm-options>-XX:+CMSClassUnloadingEnabled</jvm-options>
```

La ubicación de la configuración de JVM depende del contenedor web, como se indica en la siguiente tabla.

Tabla 15-7 Ubicación de la configuración de JVM

Contenedor Web	Archivo de configuración
Versión 2, 3 y 4 de Web Server (6.x)	<i>WebServer6-base/https-instanceName/config/server.xml</i>
Componente de producto de la Web Server (7.0)	<i>WebServer7Config-base/https-configName/config/server.xml</i>
Versión 3, 4 y 5 de Application Server (8.x)	<i>AppServer8Config-base/domains/domainName/config/domain.xml</i>
Instancia de Application Server administrada por el agente del nodo	<i>AppServer8Config-base/nodeagents/nodeagentName/config/domain.xml</i>

Deberá comprobar más adelante que no se haya modificado esta configuración de JVM como resultado del proceso de actualización de Portal Server.

Elimine la configuración del equilibrador de carga

En aquellos casos en los que se acceda a las instancias de Portal Server mediante un equilibrador de carga, el valor de la propiedad `LOAD_BALANCER_URL` que se utiliza para configurar ese acceso puede interferir en la actualización de Portal Server. Por lo tanto, debe modificarse esta configuración antes de realizar la actualización. Para modificar la configuración de la propiedad `LOAD_BALANCER_URL`:

1. Debe distinguir cuáles de los siguientes archivos de configuración residen de forma local (algunos de los cuales admiten componentes de Portal Server Secure Remote Access que pueden instalarse localmente):
PortalServer6Config-base/PSConfig.properties
PortalServer6Config-base/GWConfig.properties (si la puerta de enlace es local)
PortalServer6Config-base/RWPConfig.properties (si proxy Rewriter es local)
PortalServer6Config-base/NLPConfig.properties (si Netlet Proxy es local)
2. Registre el valor actual de la propiedad `LOAD_BALANCER_URL` en estos archivos de configuración.
3. Modifique el valor de la propiedad `LOAD_BALANCER_URL` para que señale a la instancia de Portal Server pertinente:
`LOAD_BALANCER_URL=portalHostName:port/portal`

Elimine la configuración de Directory Proxy Server

En aquellos casos en los que las instancias de Portal Server accedan a Directory Server mediante una instancia de Directory Proxy Server, la configuración de host y número de puerto de Directory Proxy Server debe modificarse antes de realizar la actualización y, a continuación, restablecerse a sus valores originales una vez realizada la actualización.

Para modificar la configuración adecuada:

1. Registre el valor actual de las propiedades DS_HOST y DS_PORT en el siguiente archivo de configuración de Access Manager:

AccessManagerConfig-base/config/AMConfig.properties

2. Modifique el valor de las propiedades DS_HOST y DS_PORT para que señalen directamente a la instancia de Directory Server pertinente.

Actualización de la Versión 4 de Portal Server (Solaris)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización (Solaris)

Al actualizar el software de Portal Server a la Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- Todas las instancias de Portal Server correspondientes a la misma imagen instalada de Portal Server se actualizan al mismo tiempo.
- El software de Portal Server está formado por subcomponentes que desempeñan una serie de roles diferentes, pero se actualizan todos de forma conjunta:
 - **Portal-base.** Incluye Mbeans administrativos y un software administrativo complementario, estructura de registro y software relacionado con la supervisión; todos estos componentes se incluyen en un mismo paquete.
 - **Portal Server aplicaciones web de Portal Server.** Incluye diversas aplicaciones web que se implementan en un contenedor web. Al menos, algunas de estas aplicaciones web deben ser compatibles con Access Manager y, a su vez, con Directory Server.
 - **Secure Remote Access Core.** Software que es compatible con Portal Server Secure Remote Access: algunos servlets y applets integrados en los archivos jar y algunos archivos compatibles no pueden implementarse en un contenedor web.

- La secuencia de comandos `psupgrade` detecta automáticamente los subcomponentes de Portal Server y las dependencias del contenedor web que se encuentran instalados en el equipo host. Por ejemplo, la secuencia de comandos realiza una consulta en el sistema para detectar la versión de Application Server o Web Server en la que se están implementando las aplicaciones web de Portal Server y adapta la información que solicita en función de la que puede detectar.

Procedimiento de actualización (Solaris)

El procedimiento que se describe a continuación hace referencia a Portal Server en el equipo en el que se vaya a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Si aún no ha realizado esta tarea, sincronice todos los componentes compartidos a la Versión 5.

Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#) en la página 69.

Este paso es un prerequisite necesario para ejecutar la secuencia de comandos `psupgrade`, que se describe en el [Paso 8 en la página 357](#).

3. Detenga todas las instancias de Portal Server Secure Remote Access Gateway, Rewriter Proxy o Netlet Proxy que podrían estar en ejecución de forma local.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxyd stop
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Asegúrese de que se esté ejecutando Access Manager si se ha implementado en un contenedor web distinto del contenedor en el que se haya implementado Portal Server.
5. Si aún no se está ejecutando, inicie el contenedor web en el que se haya implementado Portal Server para iniciar esta aplicación.

Web Server 6.x:

```
WebServer-base/https-instanceName/start
```

Web Server 7.0:

Admin Server--

WebServer7Config-base/admin-server/bin/startserv

Instance Server--

WebServer7Config-base/https-configName/bin/startserv

Application Server 8.x:

AppServer8-base/bin/asadmin start-domain --user admin_ID

--password password domainName

6. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade. Por ejemplo,

```
export ANT_HOME=/usr/sfw
```

```
export JAVA_HOME=/usr/jdk/entsys-j2se
```

7. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

8. Ejecute la secuencia de comandos psupgrade desde la distribución de Java ES Versión 5.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
```

```
./psupgrade
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.

NOTA Si ejecuta accidentalmente psupgrade desde el directorio *os_arch* incorrecto, deberá anular el procedimiento de la siguiente forma:

- a. Acceda al directorio *os_arch* correcto.

- b. Invierta los cambios efectuados en los datos de Portal Server.

```
./psupgrade rollback
```

Proporcione las contraseñas y los parámetros necesarios.

- c. Ejecute psupgrade una vez más.

La secuencia de comandos psupgrade detecta los paquetes de traducción y los componentes de Portal Server instalados, llama al programa de instalación de Java ES para instalar los nuevos paquetes y realiza una consulta en el sistema para detectar la ubicación, el número de puerto y otros datos acerca del

contenedor web en el que se vayan a implementar las aplicaciones web de Portal Server. En función del escenario de actualización del contenedor web, (consulte la [Tabla 15-4 en la página 344](#)), la secuencia de comandos le solicitará que introduzca la información adicional necesaria para implementar Portal Server en el contenedor web adecuado.

La [Tabla 15-6 en la página 351](#) muestra la información solicitada para los diferentes escenarios de actualización del contenedor web, incluidos en la [Tabla 15-4](#).

NOTA Asegúrese de introducir los valores correctos para los parámetros de `psupgrade`, ya que no se puede retroceder para cambiarlos y, además, es muy difícil deshacer los cambios efectuados por la secuencia de comandos `psupgrade`. Para invertir los cambios realizados en los datos de Portal Server, debe ejecutar

```
./psupgrade rollback
```

antes de intentar ejecutar de nuevo `psupgrade`.

9. Si es necesario, restablezca la configuración de JVM del contenedor web.

Para asegurarse de que la configuración de JVM admita la Versión 5 de Portal Server, realice los siguientes pasos:

- a. Compruebe que la configuración de JVM del contenedor web para Portal Server que se ha registrado antes de realizar la actualización no se haya modificado como resultado del proceso de actualización.

Consulte el “[Registre la configuración de la Máquina virtual de Java \(JVM\)](#)” en la [página 353](#).

- b. Si se ha modificado la configuración, restablézcala a los valores registrados antes de realizar la actualización.

Asegúrese de que se incluya la siguiente configuración de JVM, aunque no se haya establecido anteriormente:

```
<jvm-options>-XX:MaxPermSize=256m</jvm-options>
<jvm-options>-XX:+CMSPermGenSweepingEnabled</jvm-options>
<jvm-options>-XX:+CMSClassUnloadingEnabled</jvm-options>
```

10. Detenga y reinicie el contenedor web.

Aunque no sea necesario en determinadas situaciones, al reiniciar el contenedor web, se garantiza que Portal Server se inicie de forma limpia.

- a. Detenga el contenedor web de la siguiente forma:

Web Server 6.x:

WebServer-base/https-instanceName/stop

Web Server 7.0:

Admin Server--

WebServer7Config-base/admin-server/bin/stopserv

Instance Server--

WebServer7Config-base/https-configName/bin/stopserv

Application Server 8.x:

*AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName*

- b. Reinicie el contenedor web mediante los comandos que aparecen en el [Paso 5 en la página 356](#).

Actualización de la Versión 4 de Portal Server (Linux)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización (Linux)

Al actualizar el software de Portal Server a la Versión 5, se deben tener en cuenta las mismas consideraciones que en la plataforma Solaris (consulte “[Consideraciones sobre la actualización \(Solaris\)](#)” en la página 355), excepto que, en el sistema operativo Linux, la Versión 5 de Portal Server se instala en la misma ruta que la Versión 4. Por lo tanto, la secuencia de comandos `psupgrade` elimina todos los RPM anteriores al instalar los RPM de la Versión 5.

Procedimiento de actualización (Linux)

El procedimiento que se describe a continuación hace referencia a Portal Server en el equipo en el que se vaya a realizar la actualización.

PRECAUCIÓN En Linux, la actualización de Java ES Versión 4 a la Versión 5 no se puede anular. Asegúrese de realizar una copia de seguridad del sistema *antes* de llevar a cabo el siguiente procedimiento.

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Si aún no ha realizado esta tarea, sincronice todos los componentes compartidos a la Versión 5.

Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#) en la página 69.

Este paso es un prerequisite necesario para ejecutar la secuencia de comandos `psupgrade`, que se describe en el [Paso 8 en la página 361](#).

3. Detenga todas las instancias de Portal Server Secure Remote Access Gateway, Rewriter Proxy o Netlet Proxy que podrían estar en ejecución de forma local.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxyd stop
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Asegúrese de que se esté ejecutando Access Manager si se ha implementado en un contenedor web distinto del contenedor en el que se haya implementado Portal Server.
5. Si aún no se está ejecutando, inicie el contenedor web en el que se haya implementado Portal Server para iniciar esta aplicación.

Web Server 6.x:

```
WebServer-base/https-instanceName/start
```

Web Server 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/startserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/startserv
```

Application Server 8.x:

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

6. Establezca las dos variables de entorno (`ANT_HOME` y `JAVA_HOME`) necesarias para la secuencia de comandos `psupgrade`. Por ejemplo,

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

7. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

8. Ejecute la secuencia de comandos `psupgrade` desde la distribución de Java ES Versión 5.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

donde `os_arch` coincide con su plataforma como, por ejemplo, `Linux_x86`.

La secuencia de comandos `psupgrade` detecta los paquetes de traducción y los componentes de Portal Server instalados, llama al programa de instalación de Java ES para instalar los nuevos paquetes y realiza una consulta en el sistema para detectar la ubicación, el número de puerto y otros datos acerca del contenedor web en el que se vayan a implementar las aplicaciones web de Portal Server. En función del escenario de actualización del contenedor web, (consulte la [Tabla 15-4 en la página 344](#)), la secuencia de comandos le solicitará que introduzca la información adicional necesaria para implementar Portal Server en el contenedor web adecuado.

La [Tabla 15-6 en la página 351](#) muestra la información solicitada para los diferentes escenarios de actualización del contenedor web, incluidos en la [Tabla 15-4](#).

NOTA

Asegúrese de introducir los valores correctos para los parámetros de `psupgrade`, ya que no se puede retroceder para cambiarlos y, además, es muy difícil deshacer los cambios efectuados por la secuencia de comandos `psupgrade`. Aviso: realice una copia de seguridad del sistema *antes* de ejecutar la secuencia de comandos `psupgrade`.

9. Modifique el archivo de configuración

PortalServer7Config-base/platform.conf.default.

Copie la línea en la que aparece `gateway.logging.password` del siguiente archivo, del que `psupgrade` realizó una copia de seguridad:

PortalServer6Config-base.bak/platform.conf.default

y coloque la línea en *PortalServer7Config-base/platform.conf.default.*

10. Si es necesario, restablezca la configuración de JVM del contenedor web.

Para asegurarse de que la configuración de JVM admita la Versión 5 de Portal Server, realice los siguientes pasos:

- a. Compruebe que la configuración de JVM del contenedor web para Portal Server que se ha registrado antes de realizar la actualización no se haya modificado como resultado del proceso de actualización.

Consulte el [“Registre la configuración de la Máquina virtual de Java \(JVM\)” en la página 353](#).

- b. Si se ha modificado la configuración, restablézcala a los valores registrados antes de realizar la actualización.

Asegúrese de que se incluya la siguiente configuración de JVM, aunque no se haya establecido anteriormente:

```
<jvm-options>-XX:MaxPermSize=256m</jvm-options>
<jvm-options>-XX:+CMSPermGenSweepingEnabled</jvm-options>
<jvm-options>-XX:+CMSClassUnloadingEnabled</jvm-options>
```

11. Detenga y reinicie el contenedor web.

Aunque no sea necesario en determinadas situaciones, al reiniciar el contenedor web, se garantiza que Portal Server se inicie de forma limpia.

- a. Detenga el contenedor web de la siguiente forma:

Web Server 6.x:

```
WebServer-base/https-instanceName/stop
```

Web Server 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/stopserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/stopserv
```

Application Server 8.x:

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName
```

- b. Reinicie el contenedor web mediante los comandos que aparecen en el [Paso 5 en la página 360](#).

Verificación de la actualización

Puede verificar la instalación de los paquetes de la Versión 5 mediante el siguiente comando:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Consulte la [Tabla 15-5 en la página 349](#) para obtener los valores de salida.

Para verificar la actualización completa, asegúrese que aparezca Portal Desktop y que la utilidad de administración psadmin funcione como se describe en el documento.

También puede comprobar los siguientes archivos de registro de la actualización:

```
/var/sadm/install/logs/Sun_Java_System_Portal_Server_upgrade.log*
PortalServer7Data-base/logs/admin/
PortalServer7Data-base/logs/config/
```

Tareas posteriores a la actualización de la Versión 4

Tenga en cuenta los procedimientos posteriores a la actualización necesarios para abordar las siguientes situaciones:

- [Migre los datos personalizados de web-src](#)
- [Vuelva a implementar las aplicaciones de portlet personalizadas](#)
- [Migre las aplicaciones de portlet personalizadas](#)
- [Corrija el acceso al servidor de búsqueda](#)
- [Restablezca la configuración de Directory Proxy Server](#)
- [Migre los datos personalizados de web-srcRegistre manualmente los componentes de Portal Server Secure Remote Access](#)
- [Habilite el canal URLScraper](#)
- [Cambio en la página de cierre de sesión](#)

Migre los datos personalizados de web-src

Si ha agregado datos personalizados como, por ejemplo, imágenes, archivos de javascript u otros archivos para crear portal.war en el siguiente directorio:

```
PortalServer6-base/web-src
```

debe copiar estos archivos adicionales en el directorio correspondiente de la Versión 5 de Portal Server:

```
PortalServer7-base/web-src
```

Vuelva a implementar las aplicaciones de portlet personalizadas

Si ha creado e implementado aplicaciones de portlet personalizadas, estos portlets deben implementarse de nuevo manualmente una vez completada la actualización a la Versión 5 de Portal Server. Aunque existirán entradas del perfil de visualización y se mostrará el nombre del canal, no podrá ver el contenido hasta que vuelva a implementar los portlets personalizados.

Vuelva a implementar los portlets con el siguiente comando:

```
PortalServer7-base/bin/psadmin deploy-portlet
```

Puede confirmar la nueva implementación buscando el archivo `.war` y los archivos XML correspondientes en la siguiente ubicación:

```
PortalServer7Data-base/portals/Upgraded/war
```

Migre las aplicaciones de portlet personalizadas

Las aplicaciones de portlet personalizadas basadas en la infraestructura de interfaz de usuario proporcionada por Sun Java Web Console (SJWC) deben migrarse manualmente a la Versión 5 e implementarse de nuevo.

En concreto, este requisito se aplica a las cuatro aplicaciones web distribuidas con Portal Server como aplicaciones de portlet de ejemplo destinadas a personalizarse e instalarse en un portal: `filesharing`, `surveys`, `wiki`, `rssportlet`. Durante la actualización, las versiones de estas aplicaciones de portlet de ejemplo cuyos errores se han solucionado se ubican en el área de aplicaciones de portlet del disco. Si ha personalizado estas aplicaciones de portlet para su propio uso, deberá migrarlas manualmente a la Versión 5 e implementarlas de nuevo, ya que el proceso de actualización de Portal Server no las administra.

Algunas de estas aplicaciones de ejemplo (`filesharing` y `surveys`) se implementan de forma predeterminada y están disponibles para los usuarios al crearse una comunidad.

Puede actualizar, personalizar y volver a implementar las aplicaciones de portlet basadas en SJWC mediante el siguiente procedimiento. La aplicación de portlet `filesharing` se utiliza como ejemplo:

1. Extraiga los archivos jar de la Versión 5 de SJWC.
 - a. `mkdir /tmp/lh`
 - b. `cd /tmp/lh`

- c.

```
/usr/jdk/entsys-j2se/bin/jar xvf
PortalServer7-base/portlet/communityportlets.war
WEB-INF/lib/commons-beanutils.jar
WEB-INF/lib/commons-collections-3.1.jar
WEB-INF/lib/commons-digester.jar
WEB-INF/lib/commons-logging.jar
WEB-INF/lib/dataprovider.jar WEB-INF/lib/jsf-api.jar
WEB-INF/lib/jsf-impl.jar WEB-INF/lib/webui.jar
```
 - d. Cambie el nombre de uno de los archivos.

```
mv WEB-INF/lib/commons-collections-3.1.jar
WEB-INF/lib/commons-collections.jar
```
 2. Encuentre la aplicación de portlet filesharing.

```
cd PortalServer7Config-base/portals/portal1/portletapps/filesharing
```
 3. Incluya las bibliotecas de SJWC actualizadas.

```
jar uvf src/filesharing.war.tokenized -C /tmp/lh WEB-INF
```
 4. Personalice la aplicación de portlet filesharing.

```
ant customize
```
 5. Vuelva a implementar la aplicación de portlet filesharing.
 - a.

```
PortalServer7-base/bin/psadmin undeploy-portlet -u amadmin
-f passwordfile -p portal_id -i instance_id -g filesharing
```
 - b.

```
ant deploy
```
 - c. Acceda al siguiente directorio (en función del contenedor web):

Application Server 8.x:

```
AppServer8Config-base/domains/domain1/applications/j2ee-modules/
communityportlets/WEB-INF
```


Web Server 6.x:

```
WebServer6-base/https-instanceName/webapps/https-instanceName/
communityportlets/WEB-INF
```


Web Server 7.x:

```
WebServer7Config-base/https-configName/web-app/https-configName/
communityportlets/WEB-INF
```

- d. Abra el archivo `sun-web.xml` y agregue la siguiente línea justo antes de la última línea (es decir, delante de la etiqueta final `sun-web-app`):


```
<class-loader delegate="false"/>
```
- e. Repita el [Paso c](#) y el [Paso d](#) para el archivo `sun-web.xml` ubicado en `filesharing/WEB-INF`.
6. Repita del [Paso 2](#) al [Paso 5](#) para la aplicación `surveys` y las demás aplicaciones de portlet personalizadas basadas en la estructura de SJWC.
7. Reinicie el contenedor web.

Corrija el acceso al servidor de búsqueda

Al actualizar la Versión 4 de Portal Server a la Versión 5, el servidor de búsqueda se separa de Portal Server y, por lo tanto, se cambia la URL de acceso al servidor de búsqueda.

- En la Versión 4, la URL es `http://hostName:port/portal/search`
- En la Versión 5, la URL es `http://hostName:port/UpgradedSearch/search`

Por lo tanto, debe modificar manualmente los perfiles de visualización de todos los canales del portal que implementen las interfaces "SearchProvider" o "DiscussionProvider" como por ejemplo, "Search", "DiscussionLite", "Discussions" y el canal de Instant Messaging. En concreto, debe modificar la propiedad `searchServer` de estos canales en cualquier nivel de rol u organizativo en los que aparezca dentro del perfil de visualización para que haga referencia correctamente al servidor de búsqueda. Modifique el valor de `searchServer` de la siguiente forma:

```
value="http://hostName:port/UpgradedSearch/search"
```

Además, para el canal de Instant Messaging, debe actualizarse la propiedad de configuración del servidor de Instant Messaging, `im_arch.portal.search`, con la nueva URL del servidor de búsqueda.

Restablezca la configuración de Directory Proxy Server

Si las instancias de Portal Server han accedido a Directory Server mediante una instancia de Directory Proxy Server, debe restablecerse la configuración de host y número de puerto de Directory Proxy Server a los valores originales que presentaban antes de la actualización. Consulte la sección ["Elimine la configuración de Directory Proxy Server" en la página 355](#), en la que se modificaron los valores de estas propiedades como preparación para la actualización.

Registre manualmente los componentes de Portal Server Secure Remote Access

Si detecta que se ha incluido en la salida estándar una excepción de puntero nulo al final de proceso de actualización, esto quiere decir que el registro de los componentes de Portal Server Secure Remote Access (si hay alguno) ha fallado:

En ese caso, puede registrar (habilitar) manualmente los componentes de Portal Server Secure Remote Access ejecutando el siguiente comando:

```
PortalServer7-base/bin/psadmin provision-sra -u amadminUser -f passwordFile
-p Portal_ID --gateway-profile profileName --enable
```

Habilite el canal URLScrapper

Al actualizar de la Versión 4 a la Versión 5, debe habilitar el canal URLScrapper. Utilice el siguiente procedimiento:

1. Inicie una sesión en la consola de Portal Server.

Haga clic en la ficha Portal y, a continuación, en el portal actualizado.

2. En el menú desplegable Seleccionar DN, seleccione Nivel superior (Global) y haga clic en el vínculo Descargar perfil de visualización.

Almacene el archivo descargado en una ubicación temporal.

3. Encuentre `com.sun.portal.providers.urlscrapper.URLScrapperProvider`.

4. Encuentre la parte de XML que empieza por:

```
<Provider advanced="false"
class="com.sun.portal.providers.urlscrapper.URLScrapperProvider"

y termina por:
</Provider>
```

5. Sustituya la parte de XML del [Paso 4](#) por lo siguiente:

```
<Provider advanced="false"
class="com.sun.portal.providers.urlscrapper.URLScrapperProvider"
container="false" lock="false" merge="fuse"
name="URLScrapperProvider" version="2">

<Properties advanced="false" lock="false" merge="fuse"
name="_properties" propagate="true">

<String advanced="false" lock="false" merge="replace" name="title"
propagate="true" value="UrlScrapper Channel"/>
```

```

<String advanced="false" lock="false" merge="replace"
name="description" propagate="true" value="This is a test for
urlscraper"/>

<Boolean advanced="true" lock="false" merge="replace"
name="isEditable" propagate="true" value="false"/>

<Boolean advanced="true" lock="false" merge="replace"
name="isTopLevel" propagate="true" value="false"/>

<String advanced="true" lock="false" merge="replace" name="editType"
propagate="true" value="edit_subset"/>

<Boolean advanced="true" lock="false" merge="replace"
name="enableUBT" propagate="true" value="false"/>

<String advanced="false" lock="false" merge="replace"
name="urlScraperRulesetID" propagate="true"
value="default_ruleset"/>

<String advanced="false" lock="false" merge="replace" name="width"
propagate="true" value="thick"/>

<String advanced="true" lock="false" merge="replace"
name="refreshTime" propagate="true" value="0"/>

<String advanced="true" lock="false" merge="replace" name="helpURL"
propagate="true" value="en/desktop/urlscrpr.htm"/>

<String advanced="false" lock="false" merge="replace" name="url"
propagate="true" value=""/>

<String advanced="false" lock="false" merge="replace"
name="fontFace1" propagate="true" value="Sans-serif"/>

<String advanced="false" lock="false" merge="replace"
name="productName" propagate="true" value="Sun Java™ System Portal
Server 7"/>

<Boolean advanced="false" lock="false" merge="replace"
name="cookiesToForwardAll" propagate="true" value="true"/>

<String advanced="false" lock="false" merge="replace"
name="inputEncoding" propagate="true" value="UTF-8"/>

<Collection advanced="false" lock="false" merge="fuse"
name="cookiesToForwardList" propagate="true"/>

```

```

<Integer advanced="false" lock="false" merge="replace"
name="timeout" propagate="true" value="100"/>

<String advanced="true" lock="false" merge="replace" name="formData"
propagate="true" value=""/>

<Boolean advanced="true" lock="false" merge="replace"
name="isHttpAuth" propagate="true" value="false"/>

<String advanced="true" lock="false" merge="replace" name="loginUrl"
propagate="true" value=""/>

<String advanced="true" lock="false" merge="replace"
name="loginFormData" propagate="true" value=""/>

<String advanced="true" lock="false" merge="replace" name="uid"
propagate="true" value=""/>

<String advanced="true" lock="false" merge="replace" name="password"
propagate="true" value=""/>

<ConditionalProperties advanced="false" condition="client"
lock="false" merge="fuse" propagate="true" value="HTML">

<ConditionalProperties advanced="false" condition="locale"
lock="false" merge="fuse" propagate="true" value="en">

<String advanced="true" lock="false" merge="replace" name="helpURL"
propagate="true" value="en/desktop/urlscrpr.htm"/>

<String advanced="false" lock="false" merge="replace" name="url"
propagate="true" value=""/>

</ConditionalProperties>

<String advanced="true" lock="false" merge="replace" name="helpURL"
propagate="true" value="en/desktop/urlscrpr.htm"/>

<String advanced="false" lock="false" merge="replace" name="url"
propagate="true" value=""/>

</ConditionalProperties>

<ConditionalProperties advanced="false" condition="locale"
lock="false" merge="fuse" propagate="true" value="en">

<String advanced="false" lock="false" merge="replace" name="title"
propagate="true" value="UrlScraper Channel"/>

```

```
<String advanced="false" lock="false" merge="replace"
name="description" propagate="true" value="This is a test for
urlscraper"/>

</ConditionalProperties>

</Properties>

</Provider>
```

6. Guarde y cargue el archivo modificado.

Cambio en la página de cierre de sesión

La página de cierre de sesión de la Versión 5 de Portal Server presenta cambios en relación con la anterior página de cierre de sesión de Access Manager. Tenga en cuenta que estos cambios no representan un defecto del software.

Deshacer la actualización (Solaris)

En esta sección, se describen diversas consideraciones que afectan al procedimiento que permite deshacer la actualización de Portal Server, además de una descripción del propio procedimiento.

Consideraciones sobre la anulación de la actualización (Solaris)

El procedimiento para anular la actualización a la Versión 5 consiste en restablecer la instalación de la Versión 4 en *PortalServer6-base* y volver a implementar las aplicaciones web de la Versión 4.

Procedimiento de anulación de la actualización (Solaris)

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Restablezca Directory Server al estado que presentaba antes de la actualización.

Utilice las utilidades de la GUI y la línea de comandos de copia de seguridad/restablecimiento de Directory Server. Consulte el capítulo sobre copia de seguridad y restablecimiento de Directory Server, incluido en *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

3. Detenga Portal Server deteniendo su contenedor web.

Web Server 6.x:

WebServer-base/https-instanceName/stop

Web Server 7.0:

Admin Server--

WebServer7Config-base/admin-server/bin/stopserv

Instance Server--

WebServer7Config-base/https-configName/bin/stopserv

Application Server 8.x:

*AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName*

4. Elimine los paquetes de la Versión 5 de Portal Server.

a. Inicie el programa de desinstalación de Java ES.

/var/sadm/prod/SUNWentsys5/uninstall

b. Seleccione todos los componentes instalados de Portal Server.

c. Confirme la opción de desinstalación que desee.

d. Salga del programa de desinstalación de Java ES.

5. Reinicie Portal Server reiniciando su contenedor web.

Web Server 6.x:

WebServer-base/https-instanceName/start

Web Server 7.0:

Admin Server--

WebServer7Config-base/admin-server/bin/startserv

Instance Server--

WebServer7Config-base/https-configName/bin/startserv

Application Server 8.x:

*AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName*

6. Vuelva a implementar las aplicaciones web de la Versión 4 de Portal Server mediante el siguiente comando de la distribución de Java ES Versión 5:

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade rollback
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.

El comando `psupgrade rollback` anula la implementación de las aplicaciones web de la Versión 5 de Portal Server y vuelve a implementar las aplicaciones web de la Versión 4 de Portal Server.

El comando implementa de nuevo el contenido de *PortalServer6-base/web-src* en */var/PortalServer6-base/https-hostName/deploy-dir/web-apps*. Por lo tanto, todas las personalizaciones realizadas en la aplicación web Portal Server deben efectuarse primero en */web-src* e implementarse a continuación en */web-apps*. Todos los cambios que haya realizado en */web-apps* deben repetirse en */web-src* *antes* de ejecutar el comando `psupgrade rollback` ; de lo contrario, se sobrescribirán dichos cambios.

7. Detenga y reinicie el contenedor web.

Aunque no sea necesario en determinadas situaciones, al reiniciar el contenedor web, se garantiza que Portal Server se inicie de forma limpia.

Anulación de la actualización (Linux)

Como, para actualizar a la Versión 5, es necesario eliminar los archivos binarios de la Versión 4, es muy difícil deshacer la actualización en Linux.

Un enfoque de anulación de la actualización consistiría en crear un sistema paralelo y probarlo *antes* de intentar realizar una actualización. Si necesita anular la actualización, puede restablecer este sistema paralelo.

Actualización de varias instancias

En algunas arquitecturas de implementación, Portal Server se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que las instancias de Portal Server se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Si utiliza instancias de Portal Server con equilibrado de carga, puede realizar una actualización por turnos en la que se actualicen las instancias de Portal Server secuencialmente sin necesidad de interrumpir el servicio, como se describe a continuación. Este procedimiento tiene en cuenta la siguiente limitación: La Versión 4 de Portal Server no funciona con los datos de directorios de la Versión 5 de Portal Server.

La arquitectura de implementación mostrada en la [Figura 15-1 en la página 374](#) servirá para ilustrar el procedimiento de anulación de la actualización de las instancias de la Versión 4 de Portal Server a la Versión 5.

NOTA	Para las arquitecturas que incluyan componentes de Portal Server Secure Remote Access, consulte “Actualización de varias instancias” en la página 433 .
-------------	---

En la arquitectura de la [Figura 15-1](#), se accede a varias instancias de Portal Server mediante un equilibrador de carga para proporcionar disponibilidad y escalabilidad. Las instancias de Portal Server acceden, a su vez, a las instancias de Access Manager mediante un equilibrador de carga. Las instancias de Access Manager y Access Manager SDK acceden a un directorio configurado para la repetición de varias réplicas principales (MMR). Aunque se pueden utilizar otros esquemas de repetición de Directory Server, MMR es una función representativa de los servicios de directorios escalables y de alta disponibilidad.

En la [Figura 15-1](#) se agrupan las diversas instancias de Portal Server, Access Manager y Directory Server para facilitar la explicación del proceso de actualización. Portal Server 2, representa, por ejemplo, de la segunda a un número "n" de instancias de Portal Server.

Figura 15-1 Ejemplo de arquitectura de implementación de varias instancias de Portal Server



La actualización por turnos de la Versión 4 a la Versión 5 de Portal Server se realiza de la siguiente forma:

1. Si va a realizar una actualización de la Versión 4 a la Versión 5 de Access Manager, realice una actualización por turnos, como se describe en [“Actualización de varias instancias” en la página 309](#). Tenga en cuenta que, al actualizar de la Versión 4 a la Versión 5 de Portal Server, no es necesario que actualice Access Manager de la Versión 4 a la Versión 5.
2. Configure Portal Server 2 para que señale a Directory Server 2 en lugar de a Directory Server 1.

Para mayor brevedad, al realizar los pasos posteriores “Portal Server 2” significará Portal Server 2 hasta Portal Server n.
3. Actualice Portal Server 1.

- a. Deshabilite Portal Server 1 en el Equilibrador de carga B.

Las solicitudes ya no se enrutarán a Portal Server 1.

- b. Deshabilite la función MMR de Directory Server.

Directory Server 2 ya no se sincronizará con Directory Server 1.

- c. Actualice Access Manager SDK 1B a la Versión 5.

Utilice el procedimiento descrito en [“Actualización sólo de Access Manager SDK de la Versión 4”](#) en la página 311.

- d. Actualice Portal Server 1 a la Versión 5.

Realice la actualización de la instancia de Portal Server, como se describe en [“Actualización de la Versión 4 de Portal Server”](#) en la página 348, teniendo en cuenta lo siguiente:

- Tome nota de forma especial de la siguiente tarea previa a la actualización: [“Elimine la configuración del equilibrador de carga”](#) en la página 354.
- Antes de realizar la actualización, confirme que el valor de `am.encrypted.pwd` del archivo `AccessManagerConfig-base/config/AMConfig.properties` es igual para la instancia local de Access Manager SDK que para la instancia remota asociada de Access Manager.
- Asegúrese de proporcionar un valor exclusivo que no sea nulo para el parámetro Portal Instance ID solicitado por `psupgrade` para cada instancia de Portal Server que se va a actualizar.

Los datos de Portal Server para Directory Server 1 se actualizan a la Versión 5.

- e. Habilite Portal Server 1 en el Equilibrador de carga B.

Las solicitudes se volverán a enrutar a Portal Server 1.

4. Actualice Portal Server 2.

- a. Deshabilite Portal Server 2 en el Equilibrador de carga B.

Las solicitudes ya no se enrutarán a Portal Server 2.

- b. Restablezca la configuración de Portal Server 2 para que señale a Directory Server 1.

- c.** Actualice Access Manager SDK 2B a la Versión 5.

Utilice el mismo procedimiento descrito en el [Paso c en la página 375](#).

- d.** Actualice Portal Server 2 a la Versión 5.

Utilice el mismo procedimiento descrito en el [Paso d en la página 375](#).

- e.** Habilite Portal Server 2 en el Equilibrador de carga B.

Las solicitudes se volverán a enrutar a Portal Server 2.

- 5.** Habilite la función MMR de Directory Server.

Los datos de Portal Server para Directory Server 2 se sincronizarán ahora con Directory Server 1.

Actualización de Portal Server desde Java ES Versión 3

El procedimiento de actualización del componente Portal Server de Java ES 2005Q1 (Versión 3) a la Versión 5 es igual que el procedimiento de actualización de la Versión 4 de Portal Server a la Versión 5, con las siguientes excepciones:

- [Tarea previa a la actualización de la Versión 3: actualización de las dependencias de Portal Server](#)
- [Actualización de la Versión 3 de Portal Server](#)
- [Tareas posteriores a la actualización de la Versión 3](#)
- [Actualización de varias instancias](#)

Tarea previa a la actualización de la Versión 3: actualización de las dependencias de Portal Server

Al actualizar Portal Server desde la Versión 3, debe actualizar *tanto* Access Manager como el contenedor web (Web Server o Application Server) a la Versión 4 o 5 antes de actualizar Portal Server. Además, no puede dejar ninguna dependencia en la Versión 3 ni actualizar algunas dependencias a la Versión 4 y el resto a la Versión 5. Para obtener más información, consulte [“Problemas de la actualización selectiva” en la página 343](#).

Deben actualizarse las siguientes dependencias en el orden mostrado a continuación.

1. **Componentes compartidos.** Las instrucciones para actualizar los componentes compartidos de Java ES a la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).
2. **Directory Server.** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [Capítulo 5, “Directory Server” en la página 107](#).
3. **Software de contenedor web.** Las instrucciones para actualizar Web Server o Application Server están disponibles en [Capítulo 7, “Web Server” en la página 141](#) y en [Capítulo 11, “Application Server” en la página 219](#), respectivamente.

NOTA

Al actualizar los contenedores web de terceros como, por ejemplo, los de Weblogic y WebSphere, puede interrumpirse Portal Server, ya que el proceso de actualización del contenedor sobrescribe las personalizaciones realizadas en estos contenedores para poder utilizar Portal Server.

En ese caso, debe volver a instalar y configurar Portal Server para los entornos de contenedor web actualizados.

4. **Access Manager (Access Manager SDK).** Las instrucciones para actualizar Access Manager a la Versión 5 están disponibles en el [Capítulo 14, “Access Manager” en la página 281](#).

Actualización de la Versión 3 de Portal Server

Para actualizar Portal Server de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Portal Server desde Java ES Versión 4” en la página 346](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Tareas posteriores a la actualización de la Versión 3

Al actualizar Portal Server de la Versión 3 a la Versión 5, debe realizar, además de las procedimientos posteriores a la actualización descritos en [“Tareas posteriores a la actualización de la Versión 4” en la página 363](#), los procedimientos necesarios para abordar las siguientes situaciones:

- [Suscripción a un debate](#)

Suscripción a un debate

La suscripción a un debate en una comunidad no se realizará satisfactoriamente a menos que edite las propiedades de nivel superior del perfil de visualización global para agregar la siguiente propiedad de cadena:

helpURL=en/desktop/usedesk.htm

Utilice el siguiente procedimiento:

1. Cree un archivo "snippet" XML de perfil de visualización, `helpUrl.xml`:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE DisplayProfile SYSTEM "jar://resources/psdp.dtd">
<Propiedades>
  <String name="helpURL" value="en/desktop/usedesk.htm" />
</Properties>
```

2. Ejecute las propiedades del perfil de visualización global con el siguiente comando:

```
./psadmin modify-dp -u amadminUser -f /tmp/passwordFile -p portal_ID
-m -g helpUrl.xml
```

donde la opción `-m` es necesaria para no sobrescribir todo el perfil de visualización global.

Actualización de varias instancias

En algunas arquitecturas de implementación, Portal Server se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que las instancias de Portal Server se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Si utiliza instancias de Portal Server con equilibrado de carga, puede realizar una actualización por turnos en la que se actualicen las instancias de Portal Server secuencialmente sin necesidad de interrumpir el servicio, como se describe a continuación. Este procedimiento tiene en cuenta la siguiente limitación: La Versión 3 de Portal Server no funciona con los datos de directorios de la Versión 5 de Portal Server.

Para realizar una actualización por turnos de la Versión 3 a la Versión 5 de Portal Server, siga las instrucciones que aparecen en [“Actualización de varias instancias” en la página 372](#) y sustituya la referencia a la Versión 4 por la Versión 3. Además, debe actualizar también Access Manager, como se describe en el [Paso 1 en la página 374](#).

Actualización de Portal Server desde Java ES Versión 2

En esta sección se incluye información sobre la actualización del componente Portal Server de Java ES 2004Q2 (Versión 2) a la Versión 5. El proceso es similar al de la actualización de la Versión 4 a la Versión 5 de Portal Server, a excepción de algunos cambios que se describen en las siguientes secciones:

- [Tareas previas a la actualización de la Versión 2](#)
- [Actualización de la Versión 2 de Portal Server](#)
- [Tareas posteriores a la actualización de la Versión 2](#)
- [Actualización de varias instancias](#)

Tareas previas a la actualización de la Versión 2

Las tareas previas a la actualización de la Versión 2 de Portal Server son iguales a las descritas en [“Tareas previas a la actualización de la Versión 4” en la página 349](#), a excepción de la actualización de las dependencias de Portal Server:

Al actualizar Portal Server desde la Versión 2, debe actualizar *tanto* Access Manager como el contenedor web (Web Server o Application Server) a la Versión 4 o 5 antes de actualizar Portal Server. Además, no puede dejar ninguna dependencia en la Versión 2 ni actualizar algunas dependencias a la Versión 4 y el resto a la Versión 5. Para obtener más información, consulte [“Problemas de la actualización selectiva” en la página 343](#).

En concreto, el contenedor web debe actualizarse desde la Versión 2, lo que implica que sólo se admiten los escenarios 2 y 5 de la [Tabla 15-4 en la página 344](#) al ejecutar la secuencia de comandos psupgrade.

Deben actualizarse las siguientes dependencias en el orden mostrado a continuación.

1. **Componentes compartidos.** Las instrucciones para actualizar los componentes compartidos de Java ES a la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).
2. **Directory Server.** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [“Actualización de Directory Server desde Java ES Versión 2” en la página 123](#).

3. **Software de contenedor web.** Las instrucciones para actualizar Web Server o Application Server están disponibles en [Capítulo 7, “Web Server” en la página 141](#) y en [Capítulo 11, “Application Server” en la página 219](#), respectivamente.

NOTA Al actualizar los contenedores web de terceros como, por ejemplo, los de Weblogic y WebSphere, puede interrumpirse Portal Server, ya que el proceso de actualización del contenedor sobrescribe las personalizaciones realizadas en estos contenedores para poder utilizar Portal Server. En ese caso, debe volver a instalar y configurar Portal Server para los entornos de contenedor web actualizados.

4. **Access Manager (Access Manager SDK).** Las instrucciones para actualizar Access Manager a la Versión 5 están disponibles en el [Capítulo 14, “Access Manager” en la página 281](#).

Actualización de la Versión 2 de Portal Server

El procedimiento de actualización de Portal Server de la Versión 2 a la Versión 5 depende del contenedor web en el que se implemente el software de Portal Server, como se describe en las siguientes secciones.

Actualización de la Versión 2 de Portal Server: contenedor web Web Server

Para actualizar Portal Server a la Versión 5, al implementarlo en el contenedor web Web Server, siga las instrucciones que aparecen en [“Actualización de Portal Server desde Java ES Versión 4” en la página 346](#) y sustituya toda referencia a la Versión 4 por la Versión 2.

Sin embargo, si Portal Server se implementa en la Versión 5 de Web Server (Web Server 7.0), debe realizar los siguientes pasos antes de actualizar la Versión 2 de Web Server:

1. Inicie una sesión en la consola de administración de Web Server.
2. Haga clic en Editar servidores virtuales > Aplicaciones web.
3. Elimine todas las aplicaciones web implementadas con un URI que incluya /portal o /portalsamples.
4. Haga clic en Guardar.

5. Haga clic en Implementación pendiente.

Actualización de la Versión 2 de Portal Server: contenedor web Application Server

Si se actualiza la Versión 2 de Portal Server a la Versión 5, al implementarlo en el contenedor web Application Server, se actualiza Application Server de la Versión 2 a la Versión 5.

La instancia de Application Server de la Versión 2 en la que se implementó originalmente Portal Server (*instanceName*) se migra a un agente del nodo creado por el proceso de actualización de Application Server a la Versión 5. Para actualizar Portal Server en esta instancia de Application Server actualizada, es necesario llevar a cabo los siguientes pasos:

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Si aún no ha realizado esta tarea, sincronice todos los componentes compartidos a la Versión 5.

Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).

Este paso es un prerequisite necesario para ejecutar la secuencia de comandos `psupgrade`, que se describe en el [Paso 9 en la página 384](#).

3. Detenga todas las instancias de Portal Server Secure Remote Access Gateway, Rewriter Proxy o Netlet Proxy que podrían estar en ejecución de forma local.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxyd stop
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Asegúrese de que se esté ejecutando Access Manager si se ha implementado en un contenedor web distinto del contenedor en el que se haya implementado Portal Server.
5. Si aún no se está ejecutando, inicie el contenedor web en el que se haya implementado Portal Server para iniciar esta aplicación.

- a. Si aún no se ha iniciado, inicie Domain Administration Server (DAS).

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

- b. Inicie la instancia actualizada de Application Server en la que se haya implementado Portal Server (*instanceName*), si aún no se está ejecutando esa instancia del servidor.

Para ello, inicie el agente del nodo en el que se ha migrado la instancia de Application Server actualizada:

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
--password password nodeagentName
```

En los comandos anteriores y en los pasos siguientes, se utilizan las siguientes convenciones:

- donde *nodeagentName* presenta el formato *hostName_domainName*, , pero es sólo de forma predeterminada *hostName*.
- La variable de nombre de dominio, *domainName*, predeterminada es *domain1*.
- La variable de nombre de instancia, *instanceName* , predeterminada es *server1*

6. Anule la implementación de los componentes de Portal Server.

```
AppServer8-base/bin/asadmin undeploy --user admin_ID
--password password --target instanceName portal
```

```
AppServer8-base/bin/asadmin undeploy --user admin_ID
--password password --target instanceName portletsamples
```

7. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos *psupgrade*. Por ejemplo,

Sistema operativo Solaris:

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

Sistema operativo Linux:

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

8. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

9. Ejecute la secuencia de comandos `psupgrade` desde la distribución de Java ES Versión 5.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

donde *os_arch* coincide con la plataforma como, por ejemplo, `Solaris_sparc`.

NOTA Si ejecuta accidentalmente `psupgrade` desde el directorio *os_arch* incorrecto, deberá anular el procedimiento de la siguiente forma:

- a. Acceda al directorio *os_arch* correcto.
 - b. Invierta los cambios efectuados en los datos de Portal Server.

`./psupgrade rollback`
 Proporcione las contraseñas y los parámetros necesarios.
 - c. Ejecute `psupgrade` una vez más.
-

La secuencia de comandos `psupgrade` llama al programa de instalación de Java ES para instalar los nuevos paquetes y realiza una consulta en el sistema para detectar la ubicación, el número de puerto y otros datos acerca del contenedor web en el que se vayan a implementar las aplicaciones web de Portal Server. En función del escenario de actualización del contenedor web, (consulte la [Tabla 15-4 en la página 344](#)), en este caso, el escenario 5, la secuencia de comandos le solicitará que introduzca la información adicional necesaria para implementar Portal Server en el contenedor web adecuado.

La [Tabla 15-6 en la página 351](#) muestra la información solicitada al actualizar la Versión 2 de Application Server a la Versión 5 (escenario 5).

NOTA Asegúrese de introducir los valores correctos para los parámetros de `psupgrade`, ya que no se puede retroceder para cambiarlos y, además, es muy difícil deshacer los cambios efectuados por la secuencia de comandos `psupgrade`. Para invertir los cambios realizados en los datos de Portal Server, debe ejecutar

```
./psupgrade rollback
```

antes de intentar ejecutar de nuevo `psupgrade`.

10. Detenga la instancia de Domain Administration Server (DAS) y el agente del nodo que se iniciaron en el [Paso 5 en la página 382](#).

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName
```

```
AppServer8-base/bin/asadmin stop-node-agent --user admin_ID
--password password nodeagentName
```

11. Reinicie la instancia de Domain Administration Server (DAS), el agente del nodo y la instancia del servidor que se detuvieron en el [Paso 10](#).

NOTA Asegúrese de iniciar de forma independiente el agente del nodo mediante la opción `startinstances=false` antes de iniciar la instancia del servidor, como se indica a continuación.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

```
AppServer8-base/bin/asadmin start-node-agent --port DASportNumber
--startinstances=false --user admin_ID --password password
nodeagentName
```

```
AppServer8-base/bin/asadmin start-instance --port DASportNumber
--user admin_ID --password password instanceName
```

El valor predeterminado de `DASportNumber` es 4848.

Tareas posteriores a la actualización de la Versión 2

Al actualizar Portal Server de la Versión 2 a la Versión 5, debe realizar, además de las procedimientos posteriores a la actualización descritos en [“Tareas posteriores a la actualización de la Versión 4” en la página 363](#), los procedimientos necesarios para abordar las siguientes situaciones:

- [Configuración del inicio de sesión único](#)
- [Habilite el canal URLScraper](#)
- [Elimine la entrada del servicio de la puerta de enlace](#)

Configuración del inicio de sesión único

Después de actualizar Portal Server desde la Versión 2, fallarán los canales de comunicación de Portal Desktop como, por ejemplo, Correo, Calendario y Libreta de direcciones, que utilicen la metaplantilla "ssoadapter" para acceder al servidor de servicios de fondo.

Por ejemplo, si ha modificado la metaplantilla "ssoadapter" de correo de la Versión 2, SUN-UWC-MAIL, con una configuración específica para Messaging Server y, a continuación, ha realizado una actualización a la Versión 5, existirán dos metaplantillas "ssoadapter" de SUN-UWC-MAIL: una pertenece a la Versión 2, que no se ha modificado, y la otra pertenece a la Versión 5. Observará que hay metaplantillas "ssoadapter" duplicadas en la consola de Portal Server y en la interfaz de línea de comandos de psadmin, ambas con el mismo nombre.

Los canales que utilicen las metaplantillas "ssoadapter" no podrán establecer una conexión con el servidor de servicios de fondo para recuperar los datos.

Para solucionar este problema debe recuperar los datos de la metaplantillas "ssoadapter", cambiar el nombre de las entradas duplicadas y, a continuación, sustituir los datos modificados. Utilice el siguiente procedimiento:

1. Exporte los datos de la metaplantillas "ssoadapter".

Puede usar la utilidad `amadmin` para exportar los datos de servicios de Access Manager, como se indica a continuación:

- a. Cree un archivo de solicitud de amadmin, /tmp/ssoadapter-template-gets.xml.

La utilidad usará este archivo para recuperar los datos de las metaplantillas "ssoadapter":

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
  PUBLIC "-//iPlanet//iDSAME 5.0 Admin CLI DTD//EN"
  "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<Requests>
  <SchemaRequests serviceName="SunSSOAdapterService"
    SchemaType="global">
    <GetServiceDefaultValues>
      <Attribute name="sunConfigurationTemplates" />
    </GetServiceDefaultValues>
    </SchemaRequests>
  </Requests>
```

- b. Ejecute el siguiente comando de asadmin:

```
AccessManager-base/bin/amadmin -u amadminUser -w password
-t sooadapter-templates-get.xml > /tmp/ssoadapter-templates.xml
```

La salida del comando se guarda en /tmp/ssoadapter-templates.xml.

El archivo /tmp/ssoadapter-templates.xml presenta el siguiente formato:

```
sunConfigurationTemplates=
[<ssoadapter meta-template1>, <ssoadapter meta-template2>, ...]
```

y cada metaplantilla <ssoadapter meta-template> presenta la siguiente sintaxis:

```
default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D&subType=sun-one
&enableProxyAuth=false ...
```

2. Modifique el archivo /tmp/ssoadapter-templates.xml para cambiar el nombre de las metaplantillas "ssoadapter" duplicadas.

- a. Busque cada una de las plantillas en el archivo /tmp/ssoadapter-templates.xml.

Busque la cadena default|imap:/?configName= .

- b. Sustituya los nombres de las metaplantillas "ssoadapter" duplicadas por valores exclusivos.

Por ejemplo, si hay dos metaplantillas "ssoadapter" SUN-UWC-MAIL, sustituya el valor de configName en una de ellas por SUN-UWC-MAIL2, lo que dará como resultado dos plantillas con nombres exclusivos:

```
default|imap:/?configName=SUN-UWC-MAIL ...
default|imap:/?configName=SUN-UWC-MAIL2 ...
```

- 3. Cree un archivo de solicitud de amadmin que importará las metaplantillas "ssoadapter" modificadas, sobrescribiendo los datos originales.

- a. Copie /tmp/ssoadapter-templates.xml en /tmp/ssoadapter-new-templates.xml
- b. En /tmp/ssoadapter-new-templates.xml, sustituya la cadena:

sunConfigurationTemplates=[

por:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
  PUBLIC "-//iPlanet//iDSAME 5.0 Admin CLI DTD//EN"
  "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<Requests>
  <SchemaRequests serviceName="SunSSOAdapterService"
    SchemaType="Global">
    <ModifyDefaultValues>
      <AttributeValuePair>
        <Attribute name="sunConfigurationTemplates" />
      </AttributeValuePair>
    </ModifyDefaultValues>
  </SchemaRequests>
</Requests>
```

- c. Sustituya todos los signos "&" por "&".

Por ejemplo, la línea:

```
default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&subType=sun-one&enableProxyAuth=false...
```

será:

```
default|imap:/?configName=SUN-UWC-MAIL
&amp;proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&amp;subType=sun-one&amp;enableProxyAuth=false ...
```

- d. Elimine las comas (",") al final de cada metaplantilla "ssoadapter".

- e. Incluya en cada metaplantilla "ssoadapter" una etiqueta <Value> inicial y una etiqueta </Value> final.

Por ejemplo:

```
<Value>default|imap:/?configName=SUN-UWC-MAIL
&amp;proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&amp;subType=sun-one&amp;enableProxyAuth=false ...</Value>
```

- f. Elimine el corchete final ("]") de la última metaplantilla "ssoadapter".
- g. Agregue las siguientes líneas al final del archivo:

```
</AttributeValuePair>
</ModifyDefaultValues>
</SchemaRequests>
</Requests>
```

El archivo ssoadapter-new-templates.xml resultante para la plantilla única utilizada en los pasos anteriores debería presentar el siguiente aspecto:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
  PUBLIC "-//iPlanet//iDSAME 5.0 Admin CLI DTD//EN"
  "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<Requests>
  <SchemaRequests serviceName="SunSSOAdapterService"
    SchemaType="Global">
    <ModifyDefaultValues>
      <AttributeValuePair>
        <Attribute name="sunConfigurationTemplates" />
        <Value>default|imap:/?configName=SUN-UWC-MAIL
&amp;proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&amp;subType=sun-one&amp;enableProxyAuth=false ...</Value>
      </AttributeValuePair>
    </ModifyDefaultValues>
  </SchemaRequests>
</Requests>
```

4. Importe el nuevo archivo ssoadapter-new-templates.xml.

```
AccessManager-base/bin/amadmin -u amadminUser -w password -v
-t ssoadapter-new-templates.xml
```

Ahora ya puede acceder a la ficha "ssoadapter" de la consola de Portal Server para ver los adaptadores "ssoadapter" actualizados.

Habilite el canal URLScrapper

Al actualizar de la Versión 4 a la Versión 5, debe habilitar el canal URLScrapper. Consulte el [“Habilite el canal URLScrapper” en la página 367](#).

Elimine la entrada del servicio de la puerta de enlace

La entrada del usuario amService-srapGateway debe eliminarse manualmente al actualizar Portal Server desde la Versión 2; de lo contrario, el componente de puerta de enlace de Portal Server Secure Remote Access no se iniciará una vez realizada la actualización. Lleve a cabo estos pasos:

1. Inicie una sesión en la consola de Access Manager.
2. Muestre todos los usuarios en el DN de organización.
3. Elimine el usuario amService-srapGateway.

Actualización de varias instancias

No se admiten las actualizaciones por turnos de varias instancias (consulte [“Actualización de varias instancias” en la página 372](#)) al actualizar los componentes de Portal Server de la Versión 2 a la Versión 5.

Actualización de Portal Server desde la Versión intermedia 7.0

En esta sección se incluye información sobre la actualización de Portal Server de la Versión intermedia (IFR) 7.0 2005Q4 a Java ES 5 (Versión 5).

En esta sección, se describen los siguientes temas:

- [Introducción a la actualización de la versión Portal Server IFR](#)
- [Actualización de Portal Server IFR 7.0](#)
- [Actualización de varias instancias](#)

Introducción a la actualización de la versión Portal Server IFR

Al actualizar Portal Server IFR 7.0 a la Versión 5 de Portal Server, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- Portal Server IFR no se admite en Application Server 7.x, por lo tanto no se puede aplicar el escenario de actualización 5 que aparece en la [Tabla 15-4 en la página 344](#).
- La secuencia de comandos `psupgrade` utilizada para actualizar Portal Server IFR a la Versión 5 no instala nuevos paquetes, como en el caso de una actualización desde la Versión 4. En su lugar, durante el proceso de actualización, se le solicitará que aplique las siguientes revisiones:

Tabla 15-8 Revisiones¹ para actualizar Portal Server IFR a la Versión 5

Descripción	Id. de revisión: Solaris 9 y 10	Id. de revisión: Linux
Portal Server 7.1	121465-10 (SPARC) 121466-10 (x86)	121467-10
Portal Server 7.1Traducción de	123254-02 (SPARC) 124590-02 (x86)	123255-02

1. Los números de revisiones suponen la revisión mínima necesaria para actualizar a Java ES Versión 5. Si aparecen nuevas revisiones, utilícelas en lugar de las que aparecen en la tabla.

- La secuencia de comandos de actualización de `psupgrade` no admite la actualización de Portal Server IFR a la Versión 5 para la Versión 5 de Web Server. Hay dos posibilidades:
 - Si Web Server ya se ha actualizado a la Versión 5, no puede actualizar el software de Portal Server IFR implementado en el contenedor Web Server de una versión anterior. Por lo tanto, no se admite el escenario 2 de actualización del contenedor web que se muestra en la [Tabla 15-6](#).
 - Si Web Server aún *no* se ha actualizado a la Versión 5 ni tampoco se ha actualizado Access Manager a esta versión, puede actualizar, en primer lugar, el software de Portal Server IFR de un contenedor Web Server (6.x) de una versión anterior a la Versión 5 y, posteriormente, actualizar Web Server (y Access Manager) a la Versión 5. Si este es el escenario de actualización que ha utilizado, consulte [“Actualización en la Versión 5 del contenedor web Web Server \(7.0\)” en la página 403](#) para obtener instrucciones adicionales.

Actualización de Portal Server IFR 7.0

En esta sección se describe cómo realizar una actualización de Portal Server de la Versión intermedia a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización de IFR 7](#)
- [Actualización de Portal Server IFR 7.0 \(Solaris\)](#)
- [Actualización de la versión IFR 7 de Portal Server \(Linux\)](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización de IFR 7](#)
- [Deshacer la actualización \(Solaris\)](#)
- [Anulación de la actualización \(Linux\)](#)

Tareas previas a la actualización de IFR 7

Las tareas previas a la actualización de la versión IFR son iguales a las de la actualización de la Versión 4 (consulte [“Tareas previas a la actualización de la Versión 4” en la página 349](#)), excepto por lo que se refiere a la tarea [“Obtenga las contraseñas y la información de configuración necesarias” en la página 351](#) relacionada con la información necesaria para la secuencia de comandos psupgrade.

Como Portal Server IFR no se admite en Application Server 7.x, no se puede aplicar el escenario de actualización del contenedor web 5 que aparece en la [Tabla 15-6 en la página 351](#).

Actualización de Portal Server IFR 7.0 (Solaris)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server IFR, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización de IFR 7 (Solaris)

Al actualizar Portal Server IFR a Java ES Versión 5, es preciso tener en cuenta las mismas consideraciones que al realizar la actualización de la Versión 4 (consulte [“Consideraciones sobre la actualización \(Solaris\)” en la página 355](#)).

Además, consulte los problemas descritos en [“Introducción a la actualización de la versión Portal Server IFR” en la página 391](#).

Procedimiento de actualización de IFR 7 (Solaris)

El procedimiento que se describe a continuación hace referencia a Portal Server en el equipo en el que se vaya a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

su -

2. Detenga todas las instancias de Portal Server Secure Remote Access Gateway, Rewriter Proxy o Netlet Proxy que podrían estar en ejecución de forma local.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser  
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser  
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser  
-f passwordFile -t nlproxy -N gatewayProfileName
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Asegúrese de que se esté ejecutando Access Manager si se ha implementado en un contenedor web distinto del contenedor en el que se haya implementado Portal Server.
4. Si aún no se está ejecutando, inicie el contenedor web en el que se haya implementado Portal Server para iniciar esta aplicación.

Web Server 6.x:

```
WebServer-base/https-instanceName/start
```

Web Server 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/startserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/startserv
```

Application Server 8.x:

```
AppServer8-base/bin/asadmin start-domain --user admin_ID  
--password password domainName
```

5. Obtenga los números de revisión necesarios en la [Tabla 15-8 en la página 391](#).

Utilice siempre las revisiones más recientes disponibles, a menos que se le indique que utilice una revisión específica.

Las revisiones pueden descargarse en /tmp desde:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

6. Aplique la revisión adecuada de Portal Server y, si es necesario, la revisión de traducción que aparece en la [Tabla 15-8](#).

```
patchadd /tmp/patch_ID
```

7. Confirme que las actualizaciones de las revisiones se hayan realizado satisfactoriamente:

```
showrev -p | grep patch_ID
```

Como resultado, deberían devolverse las versiones de Id. de revisión aplicadas en el [Paso 6](#).

8. En los casos en los que los paquetes de traducción se hayan actualizado en el [Paso 6](#), establezca la configuración regional de JVM de la consola de Portal Server en UTF-8.

```
export LC_ALL=ja_JP.UTF-8
export LANG=ja_JP.UTF-8
```

9. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade:

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

10. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

11. Ejecute la secuencia de comandos psupgrade.

```
cd PortalServer7-base/bin
./psupgrade
```

La secuencia de comandos psupgrade no se ejecuta desde la distribución de Java ES Versión 5 ni llama al programa de instalación de Java ES (ya se han aplicado las revisiones para los paquetes).

La secuencia de comandos realiza una consulta en el sistema para detectar la ubicación, el número de puerto y otros datos acerca del contenedor web en el que se vayan a implementar las aplicaciones web de Portal Server. En función del escenario de actualización del contenedor web, (consulte la [Tabla 15-4 en la página 344](#)), la secuencia de comandos le solicitará que introduzca la información adicional necesaria para implementar Portal Server en el contenedor web adecuado.

La [Tabla 15-6 en la página 351](#) muestra la información solicitada para los diferentes escenarios de actualización del contenedor web, incluidos en la [Tabla 15-4 en la página 344](#).

NOTA	Asegúrese de introducir los valores correctos para los parámetros de <code>psupgrade</code> , ya que no se puede retroceder para cambiarlos y, además, es muy difícil deshacer los cambios efectuados por la secuencia de comandos <code>psupgrade</code> .
-------------	---

12. Detenga y reinicie el contenedor web.

Aunque no sea necesario en determinadas situaciones, al reiniciar el contenedor web, se garantiza que Portal Server se inicie de forma limpia.

Actualización de la versión IFR 7 de Portal Server (Linux)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización de IFR 7 (Linux)

Al actualizar el software de Portal Server IFR a la Versión 5 en la plataforma Linux, es preciso tener en cuenta las mismas consideraciones que en la plataforma Solaris (consulte [“Consideraciones sobre la actualización de IFR 7 \(Solaris\)” en la página 393](#)), excepto que, al instalar las revisiones de la Versión 5 en el sistema operativo Linux, se eliminan los RPM anteriores.

Procedimiento de actualización de IFR 7 (Linux)

El procedimiento que se describe a continuación hace referencia a Portal Server en el equipo en el que se vaya a realizar la actualización.

PRECAUCIÓN	En Linux, la actualización de Portal Server IFR a la Versión 5 no se puede anular. Asegúrese de realizar una copia de seguridad del sistema <i>antes</i> de llevar a cabo el siguiente procedimiento.
-------------------	---

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Detenga todas las instancias de Portal Server Secure Remote Access Gateway, Rewriter Proxy o Netlet Proxy que podrían estar en ejecución de forma local.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t nlproxy -N gatewayProfileName
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Asegúrese de que se esté ejecutando Access Manager si se ha implementado en un contenedor web distinto del contenedor en el que se haya implementado Portal Server.
4. Si aún no se está ejecutando, inicie el contenedor web en el que se haya implementado Portal Server para iniciar esta aplicación.

Web Server 6.x:

```
WebServer-base/https-instanceName/start
```

Web Server 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/startserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/startserv
```

Application Server 8.x:

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

5. Obtenga la revisión necesaria utilizando los números de revisión y los nombres de RPM que aparecen en la [Tabla 15-8 en la página 391](#).

Utilice siempre las revisiones más recientes disponibles, a menos que se le indique que utilice una revisión específica.

Las revisiones pueden descargarse en /tmp desde:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

6. Aplique la revisión de Portal Server y, si es necesario, los RPM de traducción para Portal Server que aparecen en la [Tabla 15-8 en la página 391](#), en ese orden.

Consulte el archivo Readme (Léame) para la revisión de Portal Server, que describe cómo utilizar una secuencia de comandos para aplicar los RPM de la revisión:

```
cd /tmp
```

donde /tmp es el directorio en el que se ha descargado la revisión.

```
./upgradportalrpm
```

Las secuencias de comandos de actualización instalan los RPM.

Para la revisión de traducción, instale cada RPM con el siguiente comando:

```
rpm -Fvh patchName-version.rpm
```

7. Confirme que la actualización del parche se ha realizado con éxito:

```
rpm -qa | grep sun-portal
```

Se deberían mostrar los números de las revisiones de actualización de los RPM.

8. En los casos en los que los paquetes de traducción se hayan actualizado en el [Paso 6](#), establezca la configuración regional de JVM de la consola de Portal Server en UTF-8.

```
export LC_ALL=ja_JP.UTF-8
```

```
export LANG=ja_JP.UTF-8
```

9. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade:

```
export ANT_HOME=/opt/sun
```

```
export JAVA_HOME=/usr/jdk/entsys-j2se
```

10. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

11. Ejecute la secuencia de comandos psupgrade.

```
cd PortalServer7-base/bin
```

```
./psupgrade
```

La secuencia de comandos psupgrade no se ejecuta desde la distribución de Java ES Versión 5 ni llama al programa de instalación de Java ES (ya se han aplicado las revisiones para los paquetes).

La secuencia de comandos realiza una consulta en el sistema para detectar la ubicación, el número de puerto y otros datos acerca del contenedor web en el que se vayan a implementar las aplicaciones web de Portal Server. En función del escenario de actualización del contenedor web, (consulte la [Tabla 15-4 en la página 344](#)), la secuencia de comandos le solicitará que introduzca la información adicional necesaria para implementar Portal Server en el contenedor web adecuado.

La [Tabla 15-6 en la página 351](#) muestra la información solicitada para los diferentes escenarios de actualización del contenedor web, incluidos en la [Tabla 15-4 en la página 344](#).

NOTA Asegúrese de introducir los valores correctos para los parámetros de `psupgrade`, ya que no se puede retroceder para cambiarlos y, además, es muy difícil deshacer los cambios efectuados por la secuencia de comandos `psupgrade`.

12. Detenga y reinicie el contenedor web.

Aunque no sea necesario en determinadas situaciones, al reiniciar el contenedor web, se garantiza que Portal Server se inicie de forma limpia.

Verificación de la actualización

Puede verificar la aplicación de las revisiones para actualizar los paquetes de Portal Server a la Versión 5 mediante el siguiente comando:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Consulte la [Tabla 15-5 en la página 349](#) para obtener los valores de salida.

Para verificar la actualización completa, asegúrese que aparezca Portal Desktop y que la utilidad de administración `psadmin` funcione como se describe en el documento.

También puede comprobar los siguientes archivos de registro de la actualización en `/var/sadm/install/logs`:

- `Sun_Java_System_Portal_Server_upgrade.log`
- `Sun_Java_System_Portal_Server_upgrade.log_ant_xxx.log`

donde `xxx` puede ser `preupgrade`, `upgrade`, o `postupgrade`.

Tareas posteriores a la actualización de IFR 7

Al actualizar Portal Server de la versión IFR 7 a la Versión 5, debe realizar los procedimientos de actualización necesarios para abordar las siguientes situaciones:

- [Configuración del contenedor de agentes común](#)
- [Habilitación de Java ES Monitoring Framework](#)
- [Actualización en el contenedor web Application Server](#)
- [Actualización en la Versión 5 del contenedor web Web Server \(7.0\)](#)
- [Vuelva a implementar las aplicaciones de portlet personalizadas](#)
- [Migre las aplicaciones de portlet personalizadas](#)
- [Migración manual de los portlets basados en Struts](#)

Configuración del contenedor de agentes común

El contenedor de agentes común es un componente compartido que proporciona servicios de contenedor para los agentes de supervisión y administración de Java ES. Las herramientas administrativas de Portal Server como, por ejemplo, la consola de Portal Server y la interfaz de línea de comandos `psadmin` utilizan un conjunto de agentes de supervisión y administración que reciben la denominación conjunta de servidor de administración de Portal Server y que se implementa en el contenedor de agentes común.

Si se han actualizado los componentes compartidos de Java ES a la Versión 5 antes de realizar la actualización de Portal Server IFR 7.0, es necesario que lleve a cabo los siguientes pasos adicionales para iniciar una sesión en la Versión 5 de la consola de Portal Server y utilizar la interfaz de línea de comandos `psadmin`. (Si los componentes compartidos de Java ES *no* se han actualizado a la Versión 5 antes de realizar la actualización de Portal Server IFR 7.0, omita los siguientes pasos adicionales.)

1. Reconfigure el contenedor de agentes común.

`PortalServer7-base/bin/psconfig PortalServer7-base/samples/example2.xml`

El archivo `example2.xml` proporciona la información de reconfiguración. Debe editar, en primer lugar, el archivo `example2.xml` para proporcionar las contraseñas necesarias antes de ejecutar el comando `psconfig`. Si utiliza ubicaciones de Portal Server que no son predeterminadas, debe proporcionar también los directorios correctos.

2. Edite la ruta de clase del contenedor web para que haga referencia al contenedor de agentes común.

La ruta de clase del contenedor web contendrá una referencia a la ubicación de la versión anterior del contenedor de agentes común:

(rel4CAC-base-dir/lib/cacao_cacao.jar).

Sustituya esta referencia por la ubicación de la Versión 5:

(rel5CAC-admin-dir/lib/cacao_cacao.jar).

3. Cree el archivo de propiedades, `pasconnect.properties`, en el directorio *PortalServer7Config-base* con el siguiente par de valor y propiedad:

`pas.host=.`

4. Reinicie el contenedor de agentes común.

rel5CAC-admin-dir/bin/cacaoadm start

Habilitación de Java ES Monitoring Framework

Al habilitar Java ES Monitoring Framework (componente compartido MFWK), las herramientas administrativas de Portal Server como, por ejemplo, la consola de Portal Server y la interfaz de línea de comandos `psadmin` pueden informar de las estadísticas como, por ejemplo, el número de visitantes y los portales a los que se accede frecuentemente. Para habilitar MFWK:

1. Encuentre los siguientes dos archivos:

MFWK-base/template/jesmf/desktopmfwk.properties

MFWK-base/template/jesmf/com.sun.cmm.ps.xml

donde *MFWK-base* es la siguiente ruta:

/opt/SUNWmfwk (Solaris)

/opt/sun/mfwk (Linux)

2. Copie los dos archivos en el siguiente directorio:

PortalServer7Data-base/portals/portal_ID/config/Portal_Instance/

3. En el archivo `desktopmfwk.properties`, sustituya:

`com.sun.portal.ProductCollectionId=%PS_DIR%`

por:

`com.sun.portal.ProductCollectionId=Portal_Installed_Location`

4. Agregue los siguientes dos archivos jar:

```
MFWK-base/lib/mfwk_instrum_tk.jar  
MFWK-base/lib/mfwk_agent.jar
```

en la ruta de clase del contenedor web adecuada (el archivo `server.xml` para Web Server y el archivo `domain.xml` para Application Server)

5. Reinicie el contenedor web correspondiente.

Actualización en el contenedor web Application Server

Si Portal Server se implementa en el contenedor web Application Server, debe realizar el siguiente procedimiento adicional para volver a implementar satisfactoriamente Portal Server:

1. Encuentre la sección que define la configuración de `psconsole` en el archivo `AppServer8Config-base/domains/domainName/config/server.policy` :

2. Agregue la siguiente línea al final de esa sección:

```
permission java.lang.RuntimePermission "getProtectionDomain"
```

3. Vuelva a implementar el archivo `portal.war`.

```
PortalServer7-base/bin psadmin redeploy -p portal_ID
```

4. Reinicie la instancia de Application Server.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID  
--password passworddomainName
```

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID  
--password password nodeagentName
```

donde `nodeagentName` presenta el formato `hostName_domainName`, , pero es sólo de forma predeterminada `hostName`.

Bloqueo de las conexiones en el contenedor web Application Server

Si la instancia actualizada de Portal Server se implementa en el contenedor web Application Server, las aplicaciones del portal se pueden bloquear mientras esperan la recepción de la conexiones de Java DB. Para solucionar este problema, lleve a cabo los siguientes pasos:

1. Elimine la configuración en `PortalServer7Data-base/derby/derby.properties` para los siguientes dos parámetros:

```
derby.drda.maxThreads  
derby.drda.timeslice
```

2. Reinicie Java DB.

```
ANT_HOME/bin/ant
-DPS_CONFIG=PortalServer7Config-base/PSConfig.properties
-buildfile PortalServer7-base/lib/derby.xml
[stop-instance|start-instance]
```

donde ANT_HOME es /usr/sfw (en Solaris) y /opt/sun (en Linux).

3. Cambie los valores de configuración de Java DB para Application Server.

Mediante la consola de Application Server, cambie los valores de atributos para los siguientes recursos del conjunto de conexiones: communitymcPool, FileSharingDBPool, PointBasePool, SurveyDBPool.

Cambie los siguientes valores de atributos, como se indica a continuación:

```
Idle Timeout en 300 o más
Resource Type en javax.sql.ConnectionPoolDataSource
Datasource classname en
    org.apache.derby.jdbc.ClientConnectionPoolDataSource
```

4. Reinicie la instancia de Application Server en la que se ha implementado Portal Server.

Actualización en la Versión 5 del contenedor web Web Server (7.0)

Si ha actualizado Portal Server IFR en un Web Server que aún *no* se haya actualizado a la Versión 5 debido a que la secuencia de comandos psupgrade no admite la actualización de Portal Server IFR en la Versión 5 de Web Server (consulte [“Introducción a la actualización de la versión Portal Server IFR” en la página 391](#)), debe realizar los siguientes pasos adicionales posteriores a la actualización:

1. Actualice Web Server (y Access Manager) a la Versión 5.

2. Reconfigure el contenedor de agentes común.

Utilice el procedimiento descrito en [“Configuración del contenedor de agentes común” en la página 400](#).

3. Reconfigure los valores del contenedor Web Server necesarios para la consola de Portal Server y la interfaz de línea de comandos psadmin.

a. Abra un navegador LDAP.

Los valores de configuración se almacenan en Directory Server.

- b. En DN, busque:
sunPortalAdminPortalDomainID=defaultDomain
->sunPortalAdminPortalDomainPortalID=portal1
->sunPortalAdminPortalDomainPortalServerInstanceIn=host-port
 - c. Edite los valores como, por ejemplo InstallDir,
WebContainerInstanceDir, WebContainerType, DocRoot y otros
parámetros mostrados en la [Tabla 15-6 en la página 351](#) para que se
correspondan con los valores de la Versión 5 de Web Server (7.0).
4. Cree la instancia de la Versión 5 de Portal Server.

```
PortalServer7-base/bin/psadmin create-instance newInstance_ID
```

Si ya existe el valor de *newInstance_ID*, se generará un error, por lo que es recomendable realizar este paso antes que el [Paso 5](#) indicado a continuación.

5. Elimine la instancia de Portal Server IFR.

```
PortalServer7-base/bin/psadmin delete-instance oldInstance_ID
```

Vuelva a implementar las aplicaciones de portlet personalizadas

Si ha creado e implementado aplicaciones de portlet personalizadas, estos portlets deben implementarse de nuevo manualmente una vez completada la actualización a la Versión 5 de Portal Server. Aunque existirán entradas del perfil de visualización y se mostrará el nombre del canal, no podrá ver el contenido hasta que vuelva a implementar los portlets personalizados.

Vuelva a implementar los portlets con el siguiente comando:

```
PortalServer7-base/bin/psadmin deploy-portlet
```

Puede confirmar la nueva implementación buscando el archivo `.war` y los archivos XML correspondientes en la siguiente ubicación:

```
PortalServer7Data-base/portals/Upgraded/war
```

Migre las aplicaciones de portlet personalizadas

Las aplicaciones de portlet personalizadas basadas en la infraestructura de interfaz de usuario proporcionada por Sun Java Web Console (SJWC) deben migrarse manualmente a la Versión 5 e implementarse de nuevo.

En concreto, este requisito se aplica a las cuatro aplicaciones web distribuidas con Portal Server como aplicaciones de portlet de ejemplo destinadas a personalizarse e instalarse en un portal: `filesharing`, `surveys`, `wiki`, `rssportlet`. Durante la actualización, las versiones de estas aplicaciones de portlet de ejemplo cuyos

errores se han solucionado se ubican en el área de aplicaciones de portlet del disco. Si ha personalizado estas aplicaciones de portlet para su propio uso, deberá migrarlas manualmente a la Versión 5 e implementarlas de nuevo, ya que el proceso de actualización de Portal Server no las administra.

Algunas de estas aplicaciones de ejemplo (filesharing y surveys) se implementan de forma predeterminada y están disponibles para los usuarios al crearse una comunidad.

Puede actualizar, personalizar y volver a implementar las aplicaciones de portlet basadas en SJWC mediante el siguiente procedimiento. La aplicación de portlet filesharing se utiliza como ejemplo:

1. Extraiga los archivos jar de la Versión 5 de SJWC.
 - a. `mkdir /tmp/lh`
 - b. `cd /tmp/lh`
 - c. `/usr/jdk/entsys-j2se/bin/jar xvf`
 PortalServer7-base/portlet/communityportlets.war
 WEB-INF/lib/commons-beanutils.jar
 WEB-INF/lib/commons-collections-3.1.jar
 WEB-INF/lib/commons-digester.jar
 WEB-INF/lib/commons-logging.jar
 WEB-INF/lib/dataprovider.jar WEB-INF/lib/jsf-api.jar
 WEB-INF/lib/jsf-impl.jar WEB-INF/lib/webui.jar
 - d. Cambie el nombre de uno de los archivos.
 `mv WEB-INF/lib/commons-collections-3.1.jar`
 WEB-INF/lib/commons-collections.jar
2. Encuentre la aplicación de portlet filesharing.
 `cd PortalServer7Config-base/portals/portal1/portletapps/filesharing`
3. Incluya las bibliotecas de SJWC actualizadas.
 `jar uvf src/filesharing.war.tokenized -C /tmp/lh WEB-INF`
4. Personalice la aplicación de portlet filesharing.
 `ant customize`
5. Vuelva a implementar la aplicación de portlet filesharing.
 - a. `PortalServer7-base/bin/psadmin undeploy-portlet -u amadmin`
 `-f passwordfile -p portal_id -i instance_id -g filesharing`

- b. `ant deploy`
- c. Acceda al siguiente directorio (en función del contenedor web):

Application Server 8.x:

*AppServer8Config-base/domains/domain1/applications/j2ee-modules/
communityportlets/WEB-INF*

Web Server 6.x:

*WebServer6-base/https-instanceName/webapps/https-instanceName/
communityportlets/WEB-INF*

Web Server 7.x:

*WebServer7Config-base/https-configName/web-app/https-configName/
communityportlets/WEB-INF*

- d. Abra el archivo `sun-web.xml` y agregue la siguiente línea justo antes de la última línea (es decir, delante de la etiqueta final `sun-web-app`):

`<class-loader delegate="false"/>`
 - e. Repita el [Paso c](#) y el [Paso d](#) para el archivo `sun-web.xml` ubicado en `filesharing/WEB-INF`.
6. Repita del [Paso 2](#) al [Paso 5](#) para la aplicación `surveys` y las demás aplicaciones de portlet personalizadas basadas en la estructura de SJWC.
7. Reinicie el contenedor web.

Migración manual de los portlets basados en Struts

Si tiene portlets personalizados que utilizan código basado en la estructura Struts, estos portlets deben actualizarse manualmente para que utilicen el archivo `struts.jar` incluido en la Versión 5 de Portal Server. Utilice el siguiente procedimiento:

1. Anule la implementación de la aplicación de portlet basada en Struts.

PortalServer7-base/bin psadmin undeploy-portlet

2. Actualice el archivo `.war` con la versión correcta del archivo `struts.jar`.

*Copie PortalServer7-base/lib/struts.jar en
strutsbasedPortlet/WEB-INF/lib/struts.jar*

donde *strutsbasedPortlet* es el directorio en el que residen los archivos del portlet basado en Struts.

3. Cree un archivo `.war` del directorio *strutsbasedPortlet*.
4. Vuelva a implementar la aplicación de portlet.

PortalServer7-base/bin psadmin deploy-portlet

Deshacer la actualización (Solaris)

En esta sección, se describen diversas consideraciones que afectan al procedimiento que permite deshacer la actualización de Portal Server, además de una descripción del propio procedimiento.

Consideraciones sobre la anulación de la actualización (Solaris)

El procedimiento para anular la actualización a la Versión 5 consiste en restablecer la instalación de la versión IFR en *PortalServer7-base* y volver a implementar las aplicaciones web de la versión IFR.

Procedimiento de anulación de la actualización (Solaris)

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Restablezca Directory Server al estado que presentaba antes de la actualización.

Utilice las utilidades de la GUI y la línea de comandos de copia de seguridad/restablecimiento de Directory Server. Consulte el capítulo sobre copia de seguridad y restablecimiento de Directory Server, incluido en *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

3. Anule la implementación de las aplicaciones web de la Versión 5 de Portal Server que se volvieron a implementar durante la actualización a la Versión 5.

Use las utilidades de administración del contenedor web (la línea de comandos o la consola) para anular la implementación de los siguientes paquetes:

```
portal
psconsole
search1
wsssoportlet
guessnumber
portletsamples
```

4. Detenga Portal Server deteniendo su contenedor web.

Web Server 6.x:

WebServer-base/https-instanceName/stop

Web Server 7.0:

Admin Server--

WebServer7Config-base/admin-server/bin/stopserv

Instance Server--

WebServer7Config-base/https-configName/bin/stopserv

Application Server 8.x:

*AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName*

5. Anule la aplicación de la revisión de Portal Server 7.1 que aparece en la [Tabla 15-8](#).

patchrm patch_ID

6. Reinicie Portal Server reiniciando su contenedor web.

Web Server 6.x:

WebServer-base/https-instanceName/start

Web Server 7.0:

Admin Server--

WebServer7Config-base/admin-server/bin/startserv

Instance Server--

WebServer7Config-base/https-configName/bin/startserv

Application Server 8.x:

*AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName*

7. Vuelva a implementar las aplicaciones web de Portal Server IFR mediante los siguientes comandos:

```
cd PortalServer7-base/bin
./psupgrade rollback
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.

El comando `psupgrade rollback` anula la implementación de las aplicaciones web de la Versión 5 de Portal Server y vuelve a implementar las aplicaciones web de Portal Server IFR.

El comando implementa de nuevo el contenido de *PortalServer7-base/web-src* en */var/PortalServer7-base/https-hostName/deploy-dir/web-apps*. Por lo tanto, todas las personalizaciones realizadas en la aplicación web Portal Server deben efectuarse primero en */web-src* e implementarse a continuación en */web-apps*. Todos los cambios realizados en */web-apps* deben repetirse en */web-src* *antes* de ejecutar el comando `redeploy`; de lo contrario, se sobrescribirán dichos cambios.

8. Detenga y reinicie el contenedor web.

Aunque no sea necesario en determinadas situaciones, al reiniciar el contenedor web, se garantiza que Portal Server se inicie de forma limpia.

Anulación de la actualización (Linux)

Como, para actualizar a la Versión 5, es necesario eliminar los RPM de la versión IFR, es muy difícil deshacer la actualización en Linux.

Un enfoque de anulación de la actualización consistiría en crear un sistema paralelo y probarlo *antes* de intentar realizar una actualización. Si necesita anular la actualización, puede restablecer este sistema paralelo.

Actualización de varias instancias

En algunas arquitecturas de implementación, Portal Server se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que los componentes de Portal Server se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Si utiliza instancias de Portal Server con equilibrado de carga, puede realizar una actualización por turnos en la que se actualicen las instancias de Portal Server secuencialmente sin necesidad de interrumpir el servicio. Puede actualizar cada instancia de Portal Server mientras las demás siguen ejecutándose. Para realizar una actualización por turnos de la versión IFR a la Versión 5, siga las instrucciones que aparecen en [“Actualización de varias instancias” en la página 372](#) y sustituya la referencia a la Versión 4 por la versión IFR.

Portal Server Secure Remote Access

En este capítulo se describe cómo actualizar Portal Server Secure Remote Access a Java ES 5 (Versión 5): Sun Java System Portal Server Secure Remote Access 7.1.

Este capítulo proporciona una visión general de las consideraciones que hay que tener en cuenta para la actualización de las diferentes rutas de actualización admitidas por la Versión 5. Se tratan las actualizaciones tanto en el sistema operativo Solaris como en Linux.

- “Visión general de la actualización de Portal Server Secure Remote Access” en la página 413
- “Actualización de Portal Server Secure Remote Access desde Java ES Versión 4” en la página 418
- “Actualización de Portal Server Secure Remote Access desde Java ES Versión 3” en la página 439
- “Actualización de Portal Server Secure Remote Access desde Java ES Versión 2” en la página 441
- “Actualización de Portal Server Secure Remote Access desde la Versión intermedia 7.0” en la página 444

NOTA	Las ubicaciones de los archivos de este capítulo se especifican en relación con las rutas de directorios a las que se denomina <i>PortalServer6-base</i> y <i>PortalServer6Config-base</i> (Portal Server 6.x) y <i>PortalServer7-base</i> y <i>PortalServer7Config-base</i> (Portal Server 7.x). Debe haberse especificado, al menos, parte de estas rutas como directorio de instalación durante la instalación inicial de Portal Server. De lo contrario, el programa de instalación de Java ES asigna un valor predeterminado. Los valores predeterminados de estas rutas de directorio se muestran en la siguiente tabla.
-------------	--

Tabla 16-1 Portal Server Secure Remote Access Rutas de directorio

Variable de nombre de ruta	SO Solaris	SO Linux
<i>PortalServer6-base</i>	/opt/SUNWps	/opt/sun/portal
<i>PortalServer6Config-base</i>	/etc/opt/SUNWps	/etc/opt/sun/portal
<i>PortalServer6Data-base</i>	/var/opt/SUNWps	/var/opt/sun/portal
<i>PortalServer7-base</i>	/opt/SUNWportal	/opt/sun/portal
<i>PortalServer7Config-base</i>	/etc/opt/SUNWportal	/etc/opt/sun/portal
<i>PortalServer7Data-base</i>	/var/opt/SUNWportal	/var/opt/sun/portal

Visión general de la actualización de Portal Server Secure Remote Access

En esta sección se describen los siguientes aspectos generales de Portal Server Secure Remote Access que afectan a la actualización a Java ES 5 (Versión 5):

- [Acerca de Portal Server Secure Remote Access de Java ES Versión 5](#)
- [Guía de actualización de Portal Server Secure Remote Access](#)
- [Datos de Portal Server Secure Remote Access](#)
- [Estrategia de actualización para Portal Server Secure Remote Access](#)

Acerca de Portal Server Secure Remote Access de Java ES Versión 5

Portal Server Secure Remote Access (formado por los componentes Gateway, Rewriter Proxy y Netlet Proxy) está estrechamente ligado a Portal Server, aunque se implemente normalmente en equipos distintos de los que alojan Portal Server. Los componentes de Portal Server Secure Remote Access utilizan la misma infraestructura administrativa que Portal Server e interactúan con los servlets y applets que residen en el equipo que aloja Portal Server.

El componente Portal Server Secure Remote Access de Java ES Versión 5 representa un avance importante en relación con la Versión 4, ya que incluye una serie de nuevas mejoras y funciones. Gran parte de estos cambios se realizaron en una Versión intermedia (IFR, Interim Feature Release) posterior a la Versión 4. La Versión 5 sólo presenta ligeros cambios en las funciones en relación con la versión IFR. Para obtener información sobre las mejoras y las nuevas funciones de la versión IFR, consulte *Sun Java System Portal Server 7.1 Release Notes*, <http://docs.sun.com/doc/819-4986/6n413f365?a=view>. En concreto, se ha sustituido la interfaz administrativa de línea de comandos de la Versión 4 por el comando `psadmin`.

Guía de actualización de Portal Server Secure Remote Access

La [Tabla 16-2](#) muestra las rutas de actualización compatibles de Portal Server Secure Remote Access para Java ES Versión 5. Esta tabla hace referencia tanto al sistema operativo Solaris como a Linux.

Tabla 16-2 Rutas de actualización a Java ES 5 (Versión 5): Portal Server Secure Remote Access 7.1

Versión de Java ES	Portal Server Secure Remote Access Versión	Enfoque general	Reconfiguración necesaria
Versión intermedia (IFR)	Sun Java System Portal Server Secure Remote Access IFR 7.0 2005Q4	Actualización directa: Se realiza mediante la aplicación de revisiones y, a continuación, el uso de una secuencia de comandos de actualización.	None (Ninguna).
Versión 4	Sun Java System Portal Server Secure Remote Access 6.3.1 2005Q4	Actualización directa: Se realiza mediante una secuencia de comandos de actualización.	None (Ninguna).
Versión 3	Sun Java System Portal Server Secure Remote Access 6.3.1 2005Q1	Actualización directa: Se realiza mediante una secuencia de comandos de actualización.	None (Ninguna).
Versión 2	Sun Java System Portal Server Secure Remote Access 6.3 2004Q2	Actualización directa: Se realiza mediante una secuencia de comandos de actualización.	None (Ninguna).
Versión 1	Sun ONE Portal Server Secure Remote Access 6.2 (2003Q4)	Sin actualización directa: Aunque puede realizarse actualizando primero a la Versión 3 y, a continuación, de la Versión 3 a la Versión 5.	Datos de configuración
Versiones anteriores de Java ES		Sin actualización directa.	

Datos de Portal Server Secure Remote Access

La siguiente tabla muestra el tipo de datos que puede verse afectado por una actualización del software de Portal Server Secure Remote Access.

Tabla 16-3 Portal Server Secure Remote Access Uso de datos

Tipo de datos	Ubicación	Uso
Datos de configuración	<i>PortalServer6Config-base/</i>	Configuración de Portal Server Secure Remote Access.
Esquema de directorio	Directory Server	Portal Server Secure Remote Access depende de las configuraciones de los servicios, como Portal Desktop, y de los datos de perfil del usuario almacenados en un directorio.
Configuración de servicios		
Datos de usuario		
Datos de aplicación dinámicos	Ninguna	Portal Server Secure Remote Access no almacena de forma persistente datos de aplicación como, por ejemplo, el estado de la sesión.

Estrategia de actualización para Portal Server Secure Remote Access

La estrategia utilizada para la actualización de Portal Server Secure Remote Access depende normalmente de las diferentes consideraciones descritas en el [Capítulo 1, “Planificación de las actualizaciones”](#): ruta de actualización, dependencias entre los componentes de Java ES, actualización selectiva frente a actualización completa, implementaciones de varias instancias, etc.

En esta sección se particulariza la discusión general en torno a Portal Server Secure Remote Access presentando una serie de problemas que pueden influir en el plan de actualización de Portal Server Secure Remote Access.

Problemas de compatibilidad

La Versión 5 de Portal Server Secure Remote Access presenta cambios para la interfaz pública en el comando `psadmin` utilizado para iniciar y detener los componentes Gateway, Rewriter Proxy y Netlet Proxy. Consulte *Sun Java System Portal Server 7.1 Command-Line Reference*, <http://docs.sun.com/doc/819-5030>.

Los componentes individuales de Portal Server Secure Remote Access (incluidos Gateway, Rewriter Proxy y Netlet Proxy) no son compatibles con las versiones anteriores; deben sincronizarse todos ellos, junto con el propio componente Portal Server, en Java ES Versión 5. Este requisito se aplica tanto a los componentes locales como a los componentes distribuidos de Portal Server Secure Remote Access.

Además, existe una incompatibilidad entre las estructuras de datos de Directory Server utilizadas por la Versión 5 de Portal Server y las versiones anteriores de Portal Server. Esta incompatibilidad afecta a la actualización por turnos de varias instancias de Portal Server que utilicen los mismos datos de Directory Server.

Portal Server Secure Remote Access Dependencias

Portal Server Secure Remote Access está estrechamente ligado a Portal Server en función del software incluido en Portal Server y que se esté ejecutando en el mismo equipo que Portal Server.

Sin embargo, Portal Server Secure Remote Access también depende del resto de componentes de Java ES. Estas dependencias pueden afectar al procedimiento de actualización y reconfiguración del software de Portal Server Secure Remote Access. Por ejemplo, los cambios en las interfaces o las funciones de Portal Server Secure Remote Access pueden requerir las versiones actualizadas de los componentes de los que depende Portal Server Secure Remote Access. La actualización de dichos componentes será necesaria en función de la ruta de actualización específica.

Los componentes de Portal Server Secure Remote Access presentan relaciones de dependencia con los siguientes componentes de Java ES:

- **Componentes compartidos.** Los componentes de Portal Server Secure Remote Access presentan relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)).
- **Portal Server** Los componentes de Portal Server Secure Remote Access presentan una relación de dependencia obligatoria con Portal Server, que incluye los componentes locales necesarios para poder utilizar las funciones de Portal Server Secure Remote Access.
- **Access Manager (o Access Manager SDK).** Los componentes de Portal Server Secure Remote Access presentan una relación de dependencia obligatoria con Access Manager para proporcionar servicios de autenticación y autorización para usuarios finales, incluido el inicio de sesión único. Si Access Manager se ejecuta en un equipo remoto, Access Manager SDK debe estar disponible de forma local.

- **Directory Server.** Portal Server Secure Remote Access presenta una relación de dependencia obligatoria con Directory Server, que almacena los datos del usuario. Por lo tanto, es posible que las actualizaciones de Portal Server Secure Remote Access necesiten las extensiones del esquema de directorio.

Problemas de la actualización selectiva

Aunque Java ES Versión 5 admite generalmente la actualización selectiva de todos los componentes en un equipo, el hecho de que Portal Server Secure Remote Access esté estrechamente ligado a Portal Server implica que debe actualizarse Portal Server Secure Remote Access si se actualiza Portal Server. Del mismo modo, si se actualiza Portal Server Secure Remote Access, es necesario actualizar también Portal Server.

Por lo tanto, la actualización de Portal Server Secure Remote Access está sometida a las mismas restricciones que Portal Server (consulte Portal Server [“Problemas de la actualización selectiva” en la página 343](#)): puede actualizar Portal Server Secure Remote Access y *todas* sus dependencias de componentes de productos a la Versión 5 o actualizar únicamente Portal Server Secure Remote Access y Portal Server a la Versión 5, dejando que las demás dependencias de componentes de productos permanezcan en la Versión 4.

Actualización de Portal Server Secure Remote Access desde Java ES Versión 4

En esta sección, se incluye información sobre la actualización de Portal Server Secure Remote Access desde Java ES 2005Q4 (Versión 4) a Java ES 5 (Versión 5).

En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de la Versión 4 de Portal Server Secure Remote Access](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Portal Server Secure Remote Access de Java ES de la Versión 4 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

- **Enfoque de actualización general.** La actualización se realiza mediante una secuencia de comandos de actualización, `psupgrade`. La secuencia de comandos elimina los antiguos paquetes, instala los nuevos y migra los datos de configuración, si es necesario.
- **Dependencias de actualización.** Portal Server presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Aunque la Versión 5 de Portal Server es compatible con la Versión 4 de estos componentes compartidos, es necesario actualizarlos debido a que la secuencia de comandos `psupgrade` utilizada para actualizar Portal Server requiere la Versión 5 del componente compartido ANT.

La Versión 5 de Portal Server presenta también relaciones de dependencia con un contenedor web, Access Manager y Directory Server, como se describe en [“Portal Server Secure Remote Access Dependencias” en la página 416](#). Se admiten dos enfoques para actualizar estas dependencias (consulte [“Problemas de la actualización selectiva” en la página 417](#)):

- **Dependencias de actualización.** Portal Server Secure Remote Access presenta relaciones de dependencia con determinados componentes compartidos de Java ES (consulte la [Tabla 1-7 en la página 49](#)). Sin embargo, la Versión 5 de Portal Server Secure Remote Access es compatible con la Versión 4 de estos componentes. Por lo tanto, al actualizar Portal Server Secure Remote Access a la Versión 4, la actualización de estos componentes compartidos es completamente opcional.

Sin embargo, la Versión 5 de Portal Server Secure Remote Access presenta sólo una fuerte relación de dependencia con Portal Server. La Versión 5 de Portal Server Secure Remote Access presenta también una leve relación de dependencia con Access Manager y Directory Server, como se describe en [“Portal Server Secure Remote Access Dependencias” en la página 416](#).

Se admiten dos enfoques para actualizar estas dependencias de componentes de productos (consulte [“Problemas de la actualización selectiva” en la página 417](#)):

- Los componentes de la Versión 4 satisfacen todas las dependencias (no se actualiza *ningún* componente a la Versión 5, excepto Portal Server).
- Los componentes de la Versión 5 satisfacen todas las dependencias (se actualizan *todos* los componentes a la Versión 5).

El enfoque adoptado para Portal Server Secure Remote Access debe ser el mismo que el que se adopte para Portal Server.

- **Compatibilidad con versiones anteriores.** La Versión 5 de Portal Server Secure Remote Access es compatible con la Versión 4.
- **Anulación de la actualización.** Para anular la actualización de la Versión 4 a la Versión 5 de Portal Server Secure Remote Access, se deben restablecer los paquetes y los datos del directorio de la Versión 4.
- **Problemas de plataforma.** El enfoque de actualización general de Portal Server Secure Remote Access es idéntico tanto en el sistema operativo Solaris como en Linux. Sin embargo, la Versión 5 de Portal Server Secure Remote Access se instala en una nueva ruta en el sistema operativo Solaris mientras que, en el sistema operativo Linux, se instala en la misma ruta que la Versión 4.

Actualización de la Versión 4 de Portal Server Secure Remote Access

En esta sección se describe cómo realizar una actualización de Portal Server Secure Remote Access de Java ES Versión 4 a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización de la Versión 4](#)
- [Actualización de la Versión 4 de Portal Server Secure Remote Access \(Solaris\)](#)
- [Actualización de la Versión 4 de Portal Server Secure Remote Access \(Linux\)](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización de la Versión 4](#)
- [Deshacer la actualización \(Solaris\)](#)
- [Anulación de la actualización \(Linux\)](#)

Tareas previas a la actualización de la Versión 4

Antes de actualizar Portal Server Secure Remote Access, debe realizar las tareas siguientes:

- [Verifique la información sobre la versión actual](#)
- [Actualización de las dependencias de Portal Server Secure Remote Access](#)
- [Copia de seguridad de la información de configuración de la Versión 4 de Portal Server Secure Remote Access](#)
- [Elimine la configuración del equilibrador de carga](#)
- [Elimine la configuración de Directory Proxy Server](#)
- [Obtenga las contraseñas y la información de configuración necesarias](#)

Verifique la información sobre la versión actual

Para verificar la versión actual de Portal Server Secure Remote Access, utilice el siguiente comando:

```
PortalServer6-base/bin/version
```

Tabla 16-4 Resultados de la verificación de la versión de Portal Server Secure Remote Access

Versión de Java ES	Número de versión de Portal Server Secure Remote Access
Versión 2	6.3
Versión 3	6.3.1
Versión 4	6.3.1 ¹
Versión de IFR	7.0
Versión 5	7.1

1. La única diferencia entre la Versión 3 y la 4 es una revisión. Puede buscar las revisiones de la Versión 4 mediante el comando `showrev -p | grep patch_ID` de Solaris y el comando `rpm -qa sun-portal-core` de Linux, y comparar las versiones con las que aparecen en la *Guía de actualización de Java ES Versión 4*.

Actualización de las dependencias de Portal Server Secure Remote Access

Por lo general, se recomienda actualizar todos los componentes de Java ES de un sistema informático (y de un entorno informático) a Java ES Versión 5.

Aunque la Versión 5 de Portal Server Secure Remote Access es compatible con la Versión 4 de los componentes compartidos de Java ES, es necesario actualizar estos componentes debido a que la secuencia de comandos `psupgrade` utilizada para actualizar Portal Server Secure Remote Access requiere la Versión 5 del componente compartido ANT.

Además, Portal Server Secure Remote Access requiere la actualización de Portal Server. Sin embargo, no es necesario actualizar los demás componentes de productos de Java ES Versión 4 con los que presente relaciones de dependencia.

De hecho, el enfoque de actualización de dependencias es el mismo que el utilizado para Portal Server: si se va a actualizar alguna de las dependencias a la Versión 5, es necesario actualizar todas ellas (consulte [“Problemas de la actualización selectiva” en la página 343](#)). Sin embargo, debido a la relación de dependencia de Portal Server Secure Remote Access con Portal Server, la actualización de Portal Server se hace cargo de las dependencias de Portal Server Secure Remote Access, excepto para los componentes compartidos.

Al actualizar las dependencias de Portal Server Secure Remote Access a la Versión 5, éstas deberían actualizarse en el orden siguiente (omitiendo aquéllas que es posible que ya se hayan actualizado) antes de actualizar Portal Server Secure Remote Access.

1. **Componentes compartidos.** Las instrucciones para sincronizar los componentes compartidos de Java ES en la Versión 5 están disponibles en el [“Actualización de los componentes compartidos de Java ES” en la página 69.](#)
2. **Portal Server.** Las instrucciones para actualizar Portal Server están disponibles en el [Capítulo 15, “Portal Server” en la página 337.](#)

Copia de seguridad de la información de configuración de la Versión 4 de Portal Server Secure Remote Access

Al actualizar Portal Server Secure Remote Access a la Versión 5, no es necesario reconfigurar el software de Portal Server Secure Remote Access. Sin embargo, como medida de protección, la secuencia de comandos `psupgrade` realiza una copia de seguridad de los directorios en los que se almacena la información de configuración:

PortalServer6Config-base/

Elimine la configuración del equilibrador de carga

En aquellos casos en los que se acceda a las instancias de Portal Server Secure Remote Access mediante un equilibrador de carga, el valor de la propiedad `LOAD_BALANCER_URL` que se utiliza para configurar ese acceso puede interferir en la actualización de Portal Server Secure Remote Access. Por lo tanto, debe modificarse esta configuración antes de realizar la actualización de cualquier componente de Portal Server Secure Remote Access. Para modificar la configuración de la propiedad `LOAD_BALANCER_URL`:

1. Debe distinguir cuáles de los siguientes archivos de configuración residen de forma local (algunos de los cuales admiten componentes de Portal Server que pueden instalarse localmente):

PortalServer6Config-base/PSConfig.properties (si Portal Server es local)
PortalServer6Config-base/GWConfig.properties (si la puerta de enlace es local)
PortalServer6Config-base/RWPCConfig.properties (si proxy Rewriter es local)
PortalServer6Config-base/NLPConfig.properties (si Netlet Proxy es local)

2. Registre el valor actual de la propiedad `LOAD_BALANCER_URL` en estos archivos de configuración.
3. Modifique el valor de la propiedad `LOAD_BALANCER_URL` para que señale a la instancia de Portal Server Secure Remote Access correspondiente que se va a actualizar:

`LOAD_BALANCER_URL=hostName:port/portal`

4. Asegúrese de que las siguientes propiedades de configuración hagan referencia (si están presentes) al componente de Portal Server Secure Remote Access pertinente (y *no* al equilibrador de carga), como se muestra a continuación:

En el archivo *PortalServer6Config-base/platform.conf.default*:

```
gateway.host=Gateway_hostName
```

En los archivos *PortalServer6Config-base/GWConfig.properties* y *PortalServer6Config-base/GWConfig-default.properties*:

```
GW_HOST=Gateway_hostName
GW_IP=Gateway_hostIP
```

En los archivos *PortalServer6Config-base/RWPCConfig.properties* y *PortalServer6Config-base/RWPCConfig-default.properties*:

```
RWP_HOST=RewriterProxy_hostName
RWP_IP=RewriterProxy_hostIP
```

En los archivos *PortalServer6Config-base/NLPConfig.properties* y *PortalServer6Config-base/NLPConfig-default.properties*:

```
NLP_HOST=NetLetProxy_hostName
NLP_IP=NetLetProxy_hostIP
```

Elimine la configuración de Directory Proxy Server

En aquellos casos en los que las instancias de Portal Server Secure Remote Access accedan a Directory Server mediante una instancia de Directory Proxy Server, la configuración de host y número de puerto de Directory Proxy Server debe modificarse antes de realizar la actualización y, a continuación, restablecerse a sus valores originales una vez realizada la actualización.

Para modificar la configuración adecuada:

1. Registre el valor actual de las propiedades DS_HOST y DS_PORT en el siguiente archivo de configuración de Access Manager:

```
AccessManagerConfig-base/config/AMConfig.properties
```

2. Modifique el valor de las propiedades DS_HOST y DS_PORT para que señalen directamente a la instancia de Directory Server pertinente.

Obtenga las contraseñas y la información de configuración necesarias

En función del escenario de actualización, la secuencia de comandos psupgrade necesita que introduzca información sobre las siguientes cuentas de administración:

- Id. y contraseña de administración de Directory Server
- Id. y contraseña de administración de Access Manager
- Id. y contraseña de amldapuser de Directory Server

Actualización de la Versión 4 de Portal Server Secure Remote Access (Solaris)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server Secure Remote Access, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización (Solaris)

Al actualizar el software de Portal Server Secure Remote Access a la Versión 5, es preciso tener en cuenta las siguientes consideraciones:

- El software de Portal Server Secure Remote Access está formado por subcomponentes que desempeñan una serie de roles diferentes; éstos deben actualizarse todos de forma conjunta a la Versión 5:
 - **Portal-base.** Incluye Mbeans administrativos y un software administrativo complementario, estructura de registro y software relacionado con la supervisión; todos estos componentes se incluyen en el paquete SUNWportal-base.
 - **Aplicaciones de Secure Remote Access.** Incluye Gateway, Rewriter Proxy y Netlet Proxy. Estas aplicaciones se implementan normalmente en uno o varios equipos distintos del equipo que aloja la propia instancia de Portal Server. Las aplicaciones de Secure Remote Access no necesitan ningún contenedor web.
- Si los componentes Gateway, Rewriter Proxy y Netlet Proxy no se implementan en el mismo equipo, Rewriter Proxy y Netlet Proxy deben actualizarse antes que Gateway.
- Todos los subcomponentes de Portal Server Secure Remote Access asociados a la misma imagen instalada de Portal Server Secure Remote Access se actualizan simultáneamente si se encuentran en el equipo que se va a actualizar.
- La secuencia de comandos `psupgrade` detecta automáticamente los subcomponentes de Portal Server Secure Remote Access instalados en el equipo host y actualiza esos componentes.

Procedimiento de actualización (Solaris)

El procedimiento que se describe a continuación hace referencia al componente Portal Server Secure Remote Access que reside en el equipo en el que se va a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

```
su -
```

2. Si aún no ha realizado esta tarea, sincronice todos los componentes compartidos a la Versión 5.

Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES”](#) en la página 69.

Este paso es un prerequisite necesario para ejecutar la secuencia de comandos psupgrade, que se describe en el [Paso 8 en la página 426](#).

3. Detenga todas las instancias de Gateway, Rewriter Proxy o Netlet Proxy que se estén ejecutando localmente.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxycd stop
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Asegúrese de que Access Manager está ejecutándose.
5. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade. Por ejemplo,

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

6. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

7. Si el componente de Portal Server Secure Remote Access que va a actualizar se encuentra en una ubicación remota en relación con Portal Server, copie el archivo ejecutable `dpadmin` del equipo que aloja Portal Server en el equipo que aloja el componente de Portal Server Secure Remote Access.

El archivo ejecutable `dpadmin` puede encontrarse en la siguiente ubicación:

PortalServer7-base/SUNWps.bak/bin/dpadmin, si se ha actualizado Portal Server.

PortalServer6-base/bin/dpadmin, si aún no se ha actualizado Portal Server.

8. Ejecute la secuencia de comandos `psupgrade` desde la distribución de Java ES Versión 5.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.

La secuencia de comandos `psupgrade` llama al programa de instalación de Java ES para instalar los nuevos paquetes y solicita la siguiente información:

- Id. y contraseña de administración de Directory Server
- Id. y contraseña de administración de Access Manager
- Id. y contraseña de `amldapuser` de Directory Server

9. Inicie las instancias de Gateway, Rewriter Proxy o Netlet Proxy que se habían detenido en el [Paso 3 en la página 425](#).

```
PortalServer7-base/bin/psadmin start-sra-instance -u amadminUser
-f passwordFile --name default --type gateway
```

```
PortalServer7-base/bin/psadmin start-sra-instance -u amadminUser
-f passwordFile --name default --type nlproxy
```

```
PortalServer7-base/bin/psadmin start-sra-instance -u amadminUser
-f passwordFile --name default --type rwproxy
```

Si fallan los comandos anteriores, debe registrarse (habilitar), en primer lugar, los componentes de Portal Server Secure Remote Access:

```
PortalServer7-base/bin/psadmin provision-sra -u amadminUser
-f passwordFile -p Portal_ID --gateway-profile profileName --enable
```

Actualización de la Versión 4 de Portal Server Secure Remote Access (Linux)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server Secure Remote Access, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización (Linux)

Al actualizar el software de Portal Server Secure Remote Access a la Versión 5, se deben tener en cuenta las mismas consideraciones que en la plataforma Solaris (consulte [“Consideraciones sobre la actualización \(Solaris\)” en la página 424](#)), excepto que, en el sistema operativo Linux, la Versión 5 de Portal Server Secure Remote Access se instala en la misma ruta que la Versión 4. Por lo tanto, la secuencia de comandos `psupgrade` elimina todos los RPM anteriores al instalar los RPM de la Versión 5.

Procedimiento de actualización (Linux)

El procedimiento que se describe a continuación hace referencia a Portal Server Secure Remote Access en el equipo en el que se vaya a realizar la actualización.

PRECAUCIÓN En Linux, la actualización de Java ES Versión 4 a la Versión 5 no se puede anular. Asegúrese de realizar una copia de seguridad del sistema *antes* de llevar a cabo el siguiente procedimiento.

1. Inicie sesión como root o conviértase en superusuario.
`su -`
2. Si aún no ha realizado esta tarea, sincronice todos los componentes compartidos a la Versión 5.

Las instrucciones están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).

Este paso es un prerequisite necesario para ejecutar la secuencia de comandos `psupgrade`, que se describe en el [Paso 8 en la página 428](#).

3. Detenga todas las instancias de Gateway, Rewriter Proxy o Netlet Proxy que se estén ejecutando localmente.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxycd stop
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Asegúrese de que Access Manager esté ejecutándose.
5. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade. Por ejemplo,

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

6. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo. Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

7. Si el componente de Portal Server Secure Remote Access que va a actualizar se encuentra en una ubicación remota en relación con Portal Server, copie el archivo ejecutable dpadmin del equipo que aloja Portal Server en el equipo que aloja el componente de Portal Server Secure Remote Access.

El archivo ejecutable dpadmin puede encontrarse en la siguiente ubicación:

PortalServer7-base/SUNWps.bak/bin/dpadmin, si se ha actualizado Portal Server.

PortalServer6-base/bin/dpadmin, si aún no se ha actualizado Portal Server.

8. Ejecute la secuencia de comandos psupgrade desde la distribución de Java ES Versión 5.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

donde *os_arch* coincide con la plataforma como, por ejemplo, *Solaris_sparc*.

La secuencia de comandos psupgrade llama al programa de instalación de Java ES para instalar los nuevos paquetes y solicita la siguiente información:

- Id. y contraseña de administración de Directory Server
- Id. y contraseña de administración de Access Manager
- Id. y contraseña de amldapuser de Directory Server

Verificación de la actualización

Si el componente de Portal Server Secure Remote Access que se va a actualizar se encuentra en una ubicación remota en relación con Portal Server, puede verificar la instalación de los paquetes de la Versión 5 comprobando la información sobre la versión en el siguiente archivo:

```
PortalServer7-base/lib/PSversion.properties
```

Sin embargo, si el componente de Portal Server Secure Remote Access que se va a actualizar reside en el mismo equipo que Portal Server, puede verificar la actualización mediante el siguiente comando:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID  
-f adminpasswordfile.
```

Consulte la [Tabla 16-4 en la página 421](#) para obtener los valores de salida.

También puede comprobar los archivos de registro de la actualización en:

```
/var/sadm/install/logs/Sun_Java_System_Portal_Server_upagrede.log
```

Tareas posteriores a la actualización de la Versión 4

No hay ninguna tarea posterior a la actualización de Portal Server Secure Remote Access a la Versión 5, a excepción de las siguientes:

- [Restablezca la configuración del equilibrador de carga](#)
- [Restablezca la configuración de Directory Proxy Server](#)
- [Elimine los proveedores traducidos de la Versión 4](#)

Restablezca la configuración del equilibrador de carga

Si se ha accedido a las instancias de Portal Server Secure Remote Access mediante un equilibrador de carga, es necesario realizar los siguientes pasos después de la actualización para restablecer la configuración del equilibrador de carga:

1. Establezca los siguientes parámetros en el archivo

```
PortalServer7Config-base/platform.conf.default:
```

```
gateway.virtualhost=loadBalancer_hostName loadBalancer_hostIP  
gateway.external.ip=loadBalancer_hostIP  
gateway.dsname.agent=http\://loadBalancer_hostName\  
80/portal/RemoteConfigServlet
```

2. Establezca los siguientes parámetros en el archivo *PortalServer7Config-base/GWConfig-default.properties*.

gateway.ipaddress=Gateway_hostIP
3. Establezca los parámetros correspondientes al [Paso 1](#) y el [Paso 2](#) para Rewriter Proxy y Netlet Proxy cuando se implementen estas instancias en equipos remotos en relación con el host de Portal Server.
4. Reinicie Portal Server y las instancias de Portal Server Secure Remote Access con equilibrado de carga.

Restablezca la configuración de Directory Proxy Server

Si las instancias de Portal Server Secure Remote Access han accedido a Directory Server mediante una instancia de Directory Proxy Server, debe restablecerse la configuración de host y número de puerto de Directory Proxy Server a los valores originales que presentaban antes de la actualización. Consulte la sección [“Elimine la configuración de Directory Proxy Server” en la página 423](#), en la que se modificaron los valores de estas propiedades como preparación para la actualización.

Elimine los proveedores traducidos de la Versión 4

Los servicios de Proxylet traducidos no se cargarán hasta que se eliminen los proveedores traducidos de la Versión 4, como se indica a continuación:

1. Desplácese al directorio *PortalServer7Data-base/portals/Upgraded/desktop*.
2. Elimine todos los directorios y archivos de default_Locale, a excepción de:
 - Los archivos y directorios que ha creado (no incluidos en Portal Server Secure Remote Access)
 - El archivo *message.properties*
 - Los siguientes directorios:
 - AddressBookProvider
 - BookmarkProvider
 - CalendarProvider
 - LoginProvider
 - LotusNotesAddressBookProvider
 - LotusNotesCalendarProvider
 - LotusNotesMailProvider
 - MSExchangeAddressBookProvider
 - MSExchangeCalendarProvider
 - MSExchangeMailProvidervMailProvider
 - NotesProvider

```

PersonalNoteProvider
Register
SampleRSS
SampleURLScraper
SampleXML
TemplateEditContainerProvider
TemplateTabContainerProvider
URLScraperProvider
UWCAddressBookProvider
UserInfo
UserInfoProvider
XMLProvider
error

```

3. Reinicie el contenedor web en el que se haya implementado Portal Server.

Deshacer la actualización (Solaris)

En esta sección, se describen diversas consideraciones que afectan al procedimiento que permite deshacer la actualización de Portal Server Secure Remote Access, además de una descripción del propio procedimiento.

Consideraciones sobre la anulación de la actualización (Solaris)

El procedimiento para anular la actualización a la Versión 5 consiste en restablecer la instalación de la Versión 4 en *PortalServer6-base*.

Procedimiento de anulación de la actualización (Solaris)

1. Inicie sesión como root o conviértase en superusuario.

```
su -
```

2. Restablezca Directory Server al estado que presentaba antes de la actualización.

Utilice las utilidades de la GUI y la línea de comandos de copia de seguridad/restablecimiento de Directory Server. Consulte el capítulo sobre copia de seguridad y restablecimiento de Directory Server, incluido en *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

3. Elimine los paquetes de la Versión 5 de Portal Server Secure Remote Access.
 - a. Inicie el programa de desinstalación de Java ES.

```
/var/sadm/prod/SUNWentsys5/uninstall
```

- b.** Seleccione todos los componentes instalados de Portal Server Secure Remote Access.
 - c.** Confirme la opción de desinstalación que desee.
 - d.** Salga del programa de desinstalación de Java ES.
- 4.** Restablezca los directorios *PortalServer6-base* y *PortalServer6Config-base* a sus ubicaciones originales.

Durante la actualización, se movieron a los directorios con la extensión *.bak* .

Anulación de la actualización (Linux)

Como, para actualizar a la Versión 5, es necesario eliminar los archivos binarios de la Versión 4, es muy difícil deshacer la actualización en Linux.

Un enfoque de anulación de la actualización consistiría en crear un sistema paralelo y probarlo *antes* de intentar realizar una actualización. Si necesita anular la actualización, puede restablecer este sistema paralelo.

Actualización de varias instancias

En algunas arquitecturas de implementación, los componentes de Portal Server Secure Remote Access como, por ejemplo, la puerta de enlace, se implementan en varios sistemas informáticos para proporcionar escalabilidad y seguridad, así como para mejorar la disponibilidad. Por ejemplo, es posible que los componentes de la puerta de enlace se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Si utiliza instancias de la puerta de enlace con equilibrado de carga, puede realizar una actualización por turnos en la que se actualicen las instancias de la puerta de enlace secuencialmente sin necesidad de interrumpir el servicio, como se describe a continuación. Este procedimiento tiene en cuenta la siguiente limitación: los componentes individuales de Portal Server Secure Remote Access no son compatibles con las versiones anteriores; deben sincronizarse todos, junto con el propio Portal Server a Java ES Versión 5. Sin embargo, durante una actualización por turnos, las instancias de la Versión 4 de Portal Server Secure Remote Access pueden seguir ejecutándose mientras se actualizan las instancias de Portal Server.

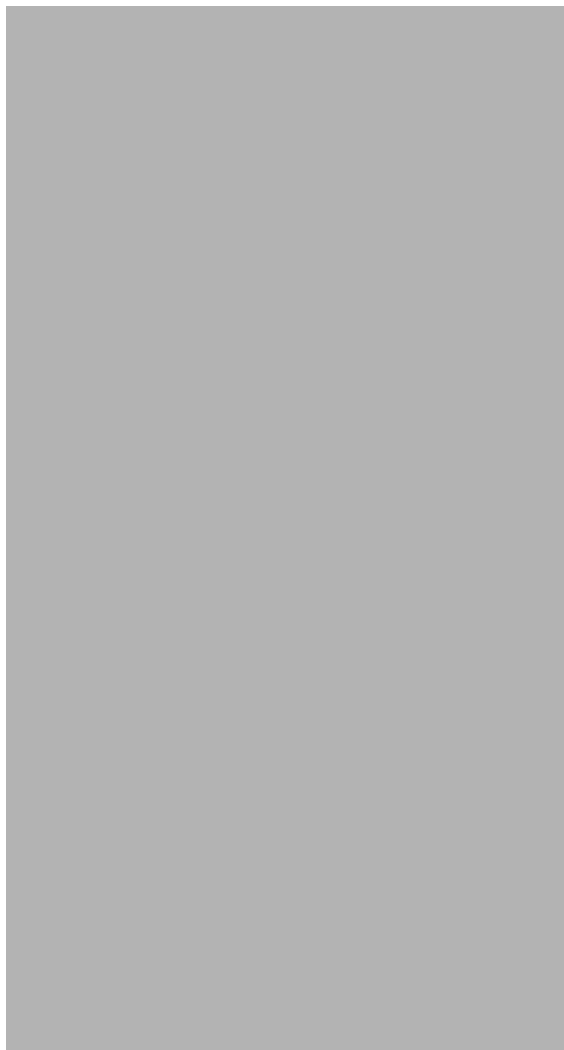
La arquitectura de implementación mostrada en la [Figura 16-1 en la página 434](#) se utilizará para ilustrar el procedimiento de actualización por turnos.

En esta arquitectura, se accede a varias instancias de Portal Server mediante las instancias de la puerta de enlace de Portal Server Secure Remote Access. Tanto las instancias de Portal Server como las de la puerta de enlace presentan equilibrado de carga para proporcionar disponibilidad y escalabilidad.

Las instancias de Portal Server acceden, a su vez, a las instancias de Access Manager mediante un equilibrador de carga. Las instancias de Access Manager y Access Manager SDK acceden a un directorio configurado para la repetición de varias réplicas principales (MMR). Aunque se pueden utilizar otros esquemas de repetición de Directory Server, MMR es una función representativa de los servicios de directorios escalables y de alta disponibilidad.

En la [Figura 16-1](#), se agrupan las diversas instancias de la puerta de enlace, Portal Server, Access Manager y Directory Server para facilitar la explicación del proceso de actualización. Portal Server 2, representa, por ejemplo, de la segunda a un número "n" de instancias de Portal Server.

Figura 16-1 Ejemplo de arquitectura de implementación de varias instancias de Portal Server



La actualización por turnos de la Versión 4 a la Versión 5 de la puerta de enlace (y Portal Server) se realiza de la siguiente forma:

1. Si va a realizar una actualización de la Versión 4 a la Versión 5 de Access Manager, realice una actualización por turnos, como se describe en [“Actualización de varias instancias” en la página 309](#). Tenga en cuenta que, al actualizar de la Versión 4 a la Versión 5 de la puerta de enlace o Portal Server, no es necesario que actualice Access Manager de la Versión 4 a la Versión 5.
2. Modifique la configuración de las instancias de Portal Server y la puerta de enlace, como se indica a continuación.
 - a. Configure Portal Server 2 para que señale a Directory Server 2 en lugar de a Directory Server 1.

Para mayor brevedad, al realizar los pasos posteriores “Portal Server 2” significará Portal Server 2 hasta Portal Server n.
 - b. Configure la Puerta de enlace 2 para que señale a Directory Server 2 en lugar de a Directory Server 1.

Para una mayor concisión, en este paso y los siguientes, “la Puerta de enlace 2” hará referencia al intervalo de la Puerta de enlace 2 a la Puerta de enlace n.
3. Actualice Portal Server 1.
 - a. Deshabilite Portal Server 1 en el Equilibrador de carga B.

Las solicitudes ya no se enrutarán a Portal Server 1.
 - b. Deshabilite la función MMR de Directory Server.

Directory Server 2 ya no se sincronizará con Directory Server 1.
 - c. Actualice Access Manager SDK 1B a la Versión 5.

Utilice el procedimiento descrito en [“Actualización sólo de Access Manager SDK de la Versión 4” en la página 311](#).
 - d. Actualice Portal Server 1 a la Versión 5.

Realice la actualización de la instancia de Portal Server, como se describe en [“Actualización de la Versión 4 de Portal Server Secure Remote Access” en la página 420](#), teniendo en cuenta lo siguiente:
 - Tome nota de forma especial de la siguiente tarea previa a la actualización: [“Elimine la configuración del equilibrador de carga” en la página 422](#).

- Antes de realizar la actualización, confirme que el valor de `am.encrypted.pwd` del archivo `AccessManagerConfig-base/config/AMConfig.properties` es igual para la instancia local de Access Manager SDK que para la instancia remota asociada de Access Manager.
- Asegúrese de proporcionar un valor exclusivo que no sea nulo para el parámetro Portal Instance ID solicitado por `psupgrade` para cada instancia de Portal Server que se va a actualizar.

Los datos de Portal Server para Directory Server 1 se actualizan a la Versión 5.

4. Actualice la Puerta de enlace 1.

- a. Deshabilite la Puerta de enlace 1 en el Equilibrador de carga C.**

Las solicitudes ya no se enrutarán a la Puerta de enlace 1.

- b. Actualice Access Manager SDK 1A a la Versión 5.**

Utilice el procedimiento descrito en [“Actualización sólo de Access Manager SDK de la Versión 4” en la página 311](#).

- c. Actualice la Puerta de enlace 1 a la Versión 5.**

Realice la actualización de puerta de enlace, como se describe en [“Actualización de la Versión 4 de Portal Server Secure Remote Access” en la página 420](#), teniendo en cuenta lo siguiente:

- Tome nota de forma especial de la siguiente tarea previa a la actualización: [“Elimine la configuración del equilibrador de carga” en la página 422](#).
- Antes de realizar la actualización, confirme que el valor de `am.encrypted.pwd` del archivo `AccessManagerConfig-base/config/AMConfig.properties` es igual para la instancia local de Access Manager SDK que para la instancia remota asociada de Access Manager.

5. Habilite los componentes deshabilitados anteriormente, Portal Server 1 y la Puerta de enlace 1 en sus respectivos equilibradores de carga, como se indica a continuación:

- a. Habilite Portal Server 1 en el Equilibrador de carga B.**

Las solicitudes se volverán a enrutar a Portal Server 1.

- b. Habilite la Puerta de enlace 1 en el Equilibrador de carga C.**

Las solicitudes se volverán a enrutar a la Puerta de enlace 1.

6. Deshabilite Portal Server 2 y la Puerta de enlace 2 en sus respectivos equilibradores de carga, como se indica a continuación:

- a. Deshabilite Portal Server 2 en el Equilibrador de carga B.

Las solicitudes ya no se enrutarán a Portal Server 2.

- b.** Deshabilite la Puerta de enlace 2 en el Equilibrador de carga C.

Las solicitudes ya no se enrutarán a la Puerta de enlace 2.

- ## 7. Actualice Portal Server 2.

- a. Restablezca la configuración de Portal Server 2 para que señale a Directory Server 1.

- b.** Actualice Access Manager SDK 2B a la Versión 5.

Utilice el procedimiento descrito en “Actualización sólo de Access Manager SDK de la Versión 4” en la página 311.

- c.** Actualice Portal Server 2 a la Versión 5.

Utilice el mismo procedimiento que en la actualización de Portal Server 1, [Paso d en la página 435](#).

- d. Habilite Portal Server 2 en el Equilibrador de carga B.**

Las solicitudes se volverán a enrutar a Portal Server 2.

- 8. Actualice la Puerta de enlace 2.**

- a. Restablezca la configuración de la Puerta de enlace 2 para que señale a Directory Server 1.

- b. Actualice Access Manager SDK 2A a la Versión 5.**

Utilice el procedimiento descrito en “Actualización sólo de Access Manager SDK de la Versión 4” en la página 311.

- c.** Actualice la Puerta de enlace 2 a la Versión 5.

Utilice el mismo procedimiento que en la actualización de la Puerta de enlace 1, [Paso c en la página 436](#).

- d.** Habilite la Puerta de enlace 2 en el Equilibrador de carga C.

Las solicitudes se volverán a enrutar a la Puerta de enlace 2.

9. Habilite la función MMR de Directory Server.

Los datos de Portal Server para Directory Server 2 se sincronizarán ahora con Directory Server 1.

NOTA En los escenarios de actualización por turnos en los que las instancias de Portal Server se actualizan a la Versión 5 mientras que permanecen activas las versiones anteriores del componente de puerta de enlace (que *no* es el caso del procedimiento anterior) y en los que se accede a las instancias de la puerta de enlace mediante un equilibrador de carga, debería comprobar que, en todas las instancias de la puerta de enlace, los archivos *PortalServer6Config-base/GWConfig.properties* y *GWConfig-default.properties* hagan referencia a la puerta de enlace y *no* al equilibrador de carga.

GW_IP=Gateway_hostIP
GW_HOST=Gateway_hostName

Si estas propiedades señalan al equilibrador de carga, la puerta de enlace ya no podrá acceder a las instancias actualizadas de Portal Server.

Actualización de Portal Server Secure Remote Access desde Java ES Versión 3

El procedimiento de actualización del componente Portal Server Secure Remote Access de Java ES 2005Q1 (Versión 3) a la Versión 5 es igual al procedimiento de actualización de la Versión 4 de Portal Server Secure Remote Access a la Versión 5, con las siguientes excepciones:

- [Actualización de las dependencias de Portal Server Secure Remote Access](#)
- [Actualización de la Versión 3 de Portal Server Secure Remote Access](#)
- [Actualización de varias instancias](#)

Actualización de las dependencias de Portal Server Secure Remote Access

Sin embargo, al actualizar Portal Server Secure Remote Access desde la Versión 3, debe actualizar Access Manager a la Versión 4 o 5 antes de actualizar Portal Server Secure Remote Access. Además, no puede dejar ninguna otra dependencia en la Versión 3 ni actualizar algunas de las dependencias a la Versión 4 y el resto a la Versión 5. Para obtener más información, consulte [“Problemas de la actualización selectiva” en la página 417](#).

Deben actualizarse las siguientes dependencias en el orden mostrado a continuación.

1. **Componentes compartidos.** Las instrucciones para actualizar los componentes compartidos de Java ES a la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#).
2. **Directory Server.** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [“Actualización de Directory Server desde Java ES Versión 2” en la página 123](#).
3. **Access Manager (Access Manager SDK).** Las instrucciones para actualizar Access Manager a la Versión 5 están disponibles en el [Capítulo 14, “Access Manager” en la página 281](#).
4. **Portal Server.** Las instrucciones para actualizar Portal Server están disponibles en el [Capítulo 15, “Portal Server” en la página 337](#).

Actualización de la Versión 3 de Portal Server Secure Remote Access

Para actualizar Portal Server Secure Remote Access de la Versión 3 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Portal Server Secure Remote Access desde Java ES Versión 4” en la página 418](#) y sustituya la referencia a la Versión 4 por la Versión 3.

Actualización de varias instancias

En algunas arquitecturas de implementación, los componentes de Portal Server Secure Remote Access como, por ejemplo, la puerta de enlace, se implementan en varios sistemas informáticos para proporcionar escalabilidad y seguridad, así como para mejorar la disponibilidad. Por ejemplo, es posible que los componentes de la puerta de enlace se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Al realizar una actualización de varias instancias de la Versión 3 de Portal Server Secure Remote Access, utilice el procedimiento que se describe en [“Actualización de varias instancias” en la página 433](#) y sustituya la referencia a la “Versión 4” por la “Versión 3”. También debe actualizar Access Manager, como se describe en el [Paso 1 en la página 435](#).

Actualización de Portal Server Secure Remote Access desde Java ES Versión 2

En esta sección se incluye información sobre la actualización del componente Portal Server Secure Remote Access de Java ES 2004Q2 (Versión 2) a la Versión 5. El proceso es similar al de la actualización de la Versión 4 a la Versión 5 de Portal Server Secure Remote Access, a excepción de algunos cambios que se describen en las siguientes secciones:

- [Tareas previas a la actualización de la Versión 2](#)
- [Actualización de la Versión 2 de Portal Server Secure Remote Access](#)
- [Tareas posteriores a la actualización de la Versión 2](#)
- [Actualización de varias instancias](#)

Tareas previas a la actualización de la Versión 2

Las tareas previas a la actualización de la Versión 2 de Portal Server Secure Remote Access son iguales a las descritas en [“Tareas previas a la actualización de la Versión 4” en la página 420](#), a excepción de las siguientes tareas:

- [Actualización de las dependencias de Portal Server Secure Remote Access](#)
- [Elimine la entrada del servicio de la puerta de enlace](#)

Actualización de las dependencias de Portal Server Secure Remote Access

Al actualizar Portal Server Secure Remote Access desde la Versión 2, debe actualizar Access Manager a la Versión 4 o 5 antes de actualizar Portal Server Secure Remote Access. Además, no puede dejar ninguna otra dependencia en la Versión 2 ni actualizar algunas de las dependencias a la Versión 4 y el resto a la Versión 5. Para obtener más información, consulte [“Problemas de la actualización selectiva” en la página 417](#).

Deben actualizarse las siguientes dependencias en el orden mostrado a continuación.

1. **Componentes compartidos.** Las instrucciones para actualizar los componentes compartidos de Java ES a la Versión 5 están disponibles en el [Capítulo 2, “Actualización de los componentes compartidos de Java ES” en la página 69](#). No obstante, si aún no se han actualizado los componentes compartidos, la secuencia de comandos `psupgrade` los actualizará automáticamente.
2. **Directory Server.** Las instrucciones para actualizar Directory Server a la Versión 5 están disponibles en el [“Actualización de Directory Server desde Java ES Versión 2” en la página 123](#).
3. **Access Manager (Access Manager SDK).** Las instrucciones para actualizar Access Manager a la Versión 5 están disponibles en el [Capítulo 14, “Access Manager” en la página 281](#).
4. **Portal Server.** Las instrucciones para actualizar Portal Server están disponibles en el [Capítulo 15, “Portal Server” en la página 337](#).

Para actualizar Portal Server Secure Remote Access de la Versión 2 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Portal Server Secure Remote Access desde Java ES Versión 4” en la página 418](#) y sustituya la referencia a la Versión 4 por la Versión 2.

Elimine la entrada del servicio de la puerta de enlace

La entrada del usuario `amService-srapGateway` debe eliminarse manualmente al actualizar Portal Server desde la Versión 2; de lo contrario, la puerta de enlace no se iniciará una vez realizada la actualización. Lleve a cabo estos pasos:

1. Inicie una sesión en la consola de Access Manager.
2. Muestre todos los usuarios en el DN de organización.
3. Elimine el usuario `amService-srapGateway`.

Actualización de la Versión 2 de Portal Server Secure Remote Access

El procedimiento de actualización del componente Portal Server Secure Remote Access de Java ES 2004Q2 (Versión 2) a la Versión 5 es igual al procedimiento de actualización de la Versión 4 de Portal Server Secure Remote Access a la Versión 5.

Para actualizar Portal Server Secure Remote Access de la Versión 2 a la Versión 5, siga las instrucciones que aparecen en [“Actualización de Portal Server Secure Remote Access desde Java ES Versión 4” en la página 418](#) y sustituya la referencia a la Versión 4 por la Versión 2.

Tareas posteriores a la actualización de la Versión 2

Las tareas posteriores a la actualización de la Versión 2 son iguales a las descritas en [“Tareas posteriores a la actualización de la Versión 4” en la página 429](#), a excepción de las siguientes tareas:

- [Establezca el dominio de Portal Server para el servicio Proxylet](#)

Establezca el dominio de Portal Server para el servicio Proxylet

Después de actualizar de la Versión 2 a la Versión 5 de Portal Server Secure Remote Access, debe establecer el valor de dominio correcto de Portal Server.

1. Inicie una sesión en la consola de Portal Server y acceda a la ficha Proxylet en Secure Remote Access.
2. Seleccione el nombre exclusivo (DN) de la organización en la que se encuentra el servicio Proxylet.
3. En el campo Dominios de las reglas de Proxylet, sustituya `SERVER_DOMAIN` por el nombre del dominio en el que se ha instalado Portal Server.
4. Repita los pasos anteriores para todas las organizaciones en las que se encuentre el servicio Proxylet.

Actualización de varias instancias

No se admiten las actualizaciones por turnos de varias instancias (consulte [“Actualización de varias instancias” en la página 433](#)) al actualizar los componentes de Portal Server Secure Remote Access (o Portal Server) de la Versión 2 a la Versión 5.

Actualización de Portal Server Secure Remote Access desde la Versión intermedia 7.0

En esta sección se incluye información sobre la actualización de Portal Server Secure Remote Access de la Versión intermedia (IFR) 7.0 2005Q4 a Java ES 5 (Versión 5).

En esta sección, se describen los siguientes temas:

- [Introducción](#)
- [Actualización de Portal Server Secure Remote Access IFR 7.0](#)
- [Actualización de varias instancias](#)

Introducción

Al actualizar Portal Server Secure Remote Access IFR 7.0 a la Versión 5, tenga en cuenta los siguientes aspectos relacionados con el proceso de actualización:

La secuencia de comandos `psupgrade` que permite actualizar Portal Server Secure Remote Access IFR a la Versión 5 no instala nuevos paquetes, como en el caso de una actualización desde la Versión 4. En su lugar, durante el proceso de actualización, se le solicitará que aplique las siguientes revisiones:

Tabla 16-5 Revisiones¹ para actualizar Portal Server Secure Remote Access IFR a la Versión 5

Descripción	Id. de revisión: Solaris 9 y 10	Id. de revisión: Linux
Portal Server 7.1	121465-10 (SPARC) 121466-10 (x86)	121467-10
Portal Server 7.1Traducción de	123254-02 (SPARC) 124590-02 (x86)	123255-02

1. Los números de revisiones suponen la revisión mínima necesaria para actualizar a Java ES Versión 5. Si aparecen nuevas revisiones, utilícelas en lugar de las que aparecen en la tabla.

Actualización de Portal Server Secure Remote Access IFR 7.0

En esta sección se describe cómo realizar una actualización de Portal Server Secure Remote Access de la Versión intermedia a Java ES Versión 5 en las plataformas Solaris y Linux. Cuando un tema haga referencia a procedimientos específicos para una plataforma, se indicará el sistema operativo al que se aplica. En esta sección, se describen los siguientes temas:

- [Tareas previas a la actualización](#)
- [Actualización de Portal Server Secure Remote Access IFR 7.0 \(Solaris\)](#)
- [Actualización de Portal Server Secure Remote Access IFR 7.0 \(Linux\)](#)
- [Verificación de la actualización](#)
- [Tareas posteriores a la actualización](#)
- [Deshacer la actualización \(Solaris\)](#)
- [Anulación de la actualización \(Linux\)](#)

Tareas previas a la actualización

Las tareas previas a la actualización de la versión IFR son iguales a las de la actualización de la Versión 4 (consulte [“Tareas previas a la actualización de la Versión 4” en la página 420](#)).

Actualización de Portal Server Secure Remote Access IFR 7.0 (Solaris)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server Secure Remote Access, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización de IFR 7 (Solaris)

Al actualizar Portal Server Secure Remote Access IFR a la Versión 5, es preciso tener en cuenta las mismas consideraciones que al realizar la actualización de la Versión 4 (consulte [“Consideraciones sobre la actualización \(Solaris\)” en la página 424](#)).

Procedimiento de actualización de IFR 7 (Solaris)

El procedimiento que se describe a continuación hace referencia a Portal Server Secure Remote Access en el equipo en el que se vaya a realizar la actualización.

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Detenga todas las instancias de Gateway, Rewriter Proxy o Netlet Proxy que se estén ejecutando localmente.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t nlproxy -N gatewayProfileName
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Asegúrese de que Access Manager esté ejecutándose.
4. Obtenga los números de revisión necesarios en la [Tabla 16-5 en la página 444](#).

Utilice siempre las revisiones más recientes disponibles, a menos que se le indique que utilice una revisión específica.

Las revisiones pueden descargarse en /tmp desde:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

5. Aplique la revisión adecuada de Portal Server y, si es necesario, la revisión de traducción que aparece en la [Tabla 16-5](#).

```
patchadd patch_ID
```

6. Confirme que la actualización de la revisión se haya realizado con éxito:

```
showrev -p | grep patch_ID
```

Como resultado, deberían devolverse las versiones de Id. de revisión aplicadas en el [Paso 5](#).

7. En los casos en los que los paquetes de traducción se hayan actualizado en el [Paso 5](#), establezca la configuración regional de JVM de la consola de Portal Server en UTF-8.

```
export LC_ALL=ja_JP.UTF-8
export LANG=ja_JP.UTF-8
```

8. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade:

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

9. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

10. Ejecute la secuencia de comandos psupgrade.

```
cd PortalServer7-base/bin
./psupgrade
```

La secuencia de comandos psupgrade no se ejecuta desde la distribución de Java ES Versión 5 ni llama al programa de instalación de Java ES (ya se han aplicado las revisiones para los paquetes).

Actualización de Portal Server Secure Remote Access IFR 7.0 (Linux)

En esta sección se abordan diversas consideraciones que afectan al proceso de actualización de Portal Server Secure Remote Access, además de una descripción del propio procedimiento.

Consideraciones sobre la actualización de IFR 7 (Linux)

Al actualizar el software de Portal Server Secure Remote Access a la Versión 5 en la plataforma Linux, es preciso tener en cuenta las mismas consideraciones que en la plataforma Solaris (consulte “[Consideraciones sobre la actualización \(Solaris\)](#)” en la [página 424](#)), excepto que, al instalar las revisiones de la Versión 5 en el sistema operativo Linux, se eliminan los RPM anteriores.

Procedimiento de actualización de IFR 7 (Linux)

El procedimiento que se describe a continuación hace referencia a Portal Server Secure Remote Access en el equipo en el que se vaya a realizar la actualización.

PRECAUCIÓN En Linux, la actualización de Portal Server Secure Remote Access IFR a la Versión 5 no se puede anular. Asegúrese de realizar una copia de seguridad del sistema *antes* de llevar a cabo el siguiente procedimiento.

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Detenga todas las instancias de Gateway, Rewriter Proxy o Netlet Proxy que se estén ejecutando localmente.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser  
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser  
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser  
-f passwordFile -t nlproxy -N gatewayProfileName
```

Compruebe que se hayan detenido los procesos. Por ejemplo:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Asegúrese de que Access Manager esté ejecutándose.
4. Obtenga la revisión necesaria utilizando los números de revisión y los nombres de RPM que aparecen en la [Tabla 16-5 en la página 444](#).

Utilice siempre las revisiones más recientes disponibles, a menos que se le indique que utilice una revisión específica.

Las revisiones pueden descargarse en /tmp desde:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

5. Aplique la revisión de Portal Server y, si es necesario, los RPM de traducción para Portal Server que aparecen en la [Tabla 16-5](#), en ese orden.

Consulte el archivo Readme (Léame) para la revisión de Portal Server, que describe cómo utilizar una secuencia de comandos para aplicar los RPM de la revisión:

```
cd /tmp
```

donde /tmp es el directorio en el que se ha descargado la revisión.

```
./update
```

Las secuencias de comandos de actualización instalan los RPM.

Para la revisión de traducción, instale cada RPM con el siguiente comando:

```
rpm -Fvh patchName-version.rpm
```

6. Confirme que la actualización del parche se ha realizado con éxito:

```
rpm -qa | grep sun-portal-core
```

Se deberían mostrar los números de las revisiones de actualización de los RPM.

7. En los casos en los que los paquetes de traducción se hayan actualizado en el [Paso 5](#), establezca la configuración regional de JVM de la consola de Portal Server en UTF-8.

```
export LC_ALL=ja_JP.UTF-8
export LANG=ja_JP.UTF-8
```

8. Establezca las dos variables de entorno (ANT_HOME y JAVA_HOME) necesarias para la secuencia de comandos psupgrade:

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entSYS-j2se
```

9. Asegúrese de que dispone del espacio de intercambio adecuado en el equipo.

Normalmente, el espacio de intercambio suele establecerse en el doble de la cantidad de memoria RAM física.

10. Ejecute la secuencia de comandos psupgrade.

```
cd PortalServer7-base/bin
./psupgrade
```

La secuencia de comandos psupgrade no se ejecuta desde la distribución de Java ES Versión 5 ni llama al programa de instalación de Java ES (ya se han aplicado las revisiones para los paquetes).

Verificación de la actualización

Puede verificar la aplicación de las revisiones para actualizar los paquetes de Portal Server Secure Remote Access a la Versión 5 mediante el siguiente comando:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Consulte la [Tabla 16-4 en la página 421](#) para obtener los valores de salida.

También puede comprobar los archivos de registro de la actualización en:

/var/sadm/install/logs/Sun_Java_System_Portal_Server_upagrede.log

Tareas posteriores a la actualización

No es necesario realizar ninguna tarea posterior a la actualización de Portal Server Secure Remote Access a la Versión 5.

Deshacer la actualización (Solaris)

En esta sección, se describen diversas consideraciones que afectan al procedimiento que permite deshacer la actualización de Portal Server Secure Remote Access, además de una descripción del propio procedimiento.

Consideraciones sobre la anulación de la actualización (Solaris)

El procedimiento para anular la actualización a la Versión 5 consiste en restablecer la instalación de la versión IFR en *PortalServer7-base*.

Procedimiento de anulación de la actualización (Solaris)

1. Inicie sesión como root o conviértase en superusuario.

`su -`

2. Restablezca Directory Server al estado que presentaba antes de la actualización.

Utilice las utilidades de la GUI y la línea de comandos de copia de seguridad/restablecimiento de Directory Server. Consulte el capítulo sobre copia de seguridad y restablecimiento de Directory Server, incluido en *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

3. Anule la aplicación de la revisión de Portal Server 7.1 que aparece en la [Tabla 16-5 en la página 444](#).

`patchrm patch_ID`

Anulación de la actualización (Linux)

En la plataforma Linux, no existe ningún procedimiento para anular la actualización.

Actualización de varias instancias

En algunas arquitecturas de implementación, Portal Server Secure Remote Access se implementa en varios sistemas informáticos para proporcionar escalabilidad y mejorar la disponibilidad. Por ejemplo, es posible que los componentes de Portal Server Secure Remote Access se ejecuten en varios equipos con un equilibrador que distribuya la carga.

Si utiliza instancias de Portal Server Secure Remote Access con equilibrado de carga, puede realizar una actualización por turnos en la que se actualicen las instancias de Portal Server Secure Remote Access secuencialmente sin necesidad de interrumpir el servicio. Puede actualizar cada instancia de Portal Server Secure Remote Access mientras las demás siguen ejecutándose. Debe realizar la actualización de cada instancia como se describe en [“Actualización de Portal Server Secure Remote Access IFR 7.0” en la página 445](#).

Al realizar una actualización de varias instancias de Portal Server Secure Remote Access IFR, utilice el procedimiento que se describe en [“Actualización de varias instancias” en la página 433](#) y sustituya la referencia a la “Versión 4” por “IFR”. También debe actualizar Access Manager, como se describe en el [Paso 1 en la página 435](#).

Contenido de las versiones de Java Enterprise System

Este apéndice muestra los contenidos de las distintas versiones de Java Enterprise System. Incluye las siguientes secciones:

- “Java ES 2003Q4 (Versión 1)” en la página 454
- “Java ES 2004Q2 (Versión 2)” en la página 456
- “Java ES 2005Q1 (Versión 3)” en la página 459
- “Java ES 2005Q4 (Versión 4)” en la página 464
- “Java ES 5 (Versión 5)” en la página 469

Java ES 2003Q4 (Versión 1)

Este apartado muestra el contenido de Java Enterprise System 2003Q4

Componentes de la Versión 1 que se pueden seleccionar en el programa de instalación

Los productos de componentes de Sun Open Network Environment (Sun ONE) y Sun Cluster aportan los servicios de infraestructura necesarios para poder utilizarlos con aplicaciones de empresa distribuidas. Estos son los productos componentes:

- Sun Cluster 3.1 y Sun Cluster Agents para Sun ONE
- Sun ONE Administration Server 5.2
- Sun ONE Application Server 7, Update 1
- Sun ONE Calendar Server 6.0
- Sun ONE Directory Server 5.2
- Sun ONE Directory Proxy Server 5.2
- Sun ONE Identity Server 6.1
- Sun ONE Instant Messaging 6.1
- Sun ONE Message Queue 3.0.1 Service Pack 2
- Sun ONE Messaging Server 6.0
- Sun ONE Portal Server 6.2
- Sun ONE Portal Server, Secure Remote Access 6.2
- Sun ONE Web Server 6.1

Componentes compartidos de la Versión 1

Los componentes compartidos proporcionan los servicios locales y la tecnología de la que dependen los productos componentes. Cuando se instalan productos componentes, el programa de instalación de Java ES instala automáticamente los componentes compartidos que se requieren, en caso de que no estén instalados.

Java Enterprise System incluye los siguientes componentes compartidos:

- ANT (herramienta de creación basada en Jakarta ANT Java/XML)
- Apache Commons Logging
- ICU (International Components for Unicode)
- J2SE™ platform 1.4.1_06 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Sun ONE Application Framework)
- JavaHelp™ Runtime
- JAXM (Java API for XML Messaging) Client Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java APIs for XML-based Remote Procedure Call)
- JSS (Java Security Services)
- KT Search Engine
- LDAP C Language SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP with Attachments API for Java)
- SASL (Simple Authentication and Security Layer)
- XML C Library (libxml)

NOTA	El sistema también requiere la instalación de Perl para Application Server y Directory Server, pero no se instala automáticamente como componente compartido de Java ES.
-------------	--

Java ES 2004Q2 (Versión 2)

Este apartado muestra el contenido de Java Enterprise System 2004Q2.

Componentes de la Versión 2 que se pueden seleccionar en el programa de instalación

Los productos componentes ofrecen los servicios de infraestructura necesarios para el uso de aplicaciones de empresa distribuidas. Al instalar Java Enterprise System en un determinado host, puede seleccionar los productos componentes que desea instalar en ese host en función de su arquitectura de implementación general.

Java Enterprise System 2004Q2 incluye los siguientes productos componentes:

Communication & Collaboration Services

- Sun Java System Messaging Server 6 2004Q2
- Sun Java System Calendar Server 6 2004Q2
- Sun Java System Instant Messaging 6 2004Q2
- Sun Java System Portal Server 2004Q2
- Sun Java System Portal Server Mobile Access 2004Q2
- Sun Java System Portal Server Secure Remote Access 2004Q2
- Sun Java System Communications Express 6 2004Q2

Web & Application Services

- Sun Java System Application Server 7.0 Update 3 (Standard Edition y Platform Edition)
- Sun Java System Web Server 6 2004Q2 Update 1 Service Pack 2
- Sun Java System Message Queue 3.5 SP1 (Platform Edition y Enterprise Edition)

Directory & Identity Services

- Sun Java System Identity Server 6.2 2004Q2, incluido
Sun Java System Communications Services 6 2004Q2 User Management Utility
- Sun Java System Directory Server 5 2004Q2
- Sun Java System Directory Proxy Server 5 2004Q2

Availability Services

- Sun Cluster 3.1 4/04 y Sun Cluster Agents para Sun Java System

Administrative Services

- Sun Java System Administration Server 5 2004T2
- Sun Remote Services Net Connect 3.5

Tenga en cuenta que Sun Cluster, Sun Cluster Agents y Sun Remote Services Net Connect no están disponibles en el sistema operativo Linux.

Componentes compartidos de la Versión 2

Los componentes compartidos proporcionan los servicios locales y la tecnología de la que dependen los productos componentes. Cuando se instalan productos componentes, el programa de instalación de Java ES instala automáticamente los componentes compartidos que se requieren, en caso de que no estén instalados.

Java Enterprise System 2004Q2 incluye los siguientes componentes compartidos:

- Ant (herramienta basada en Jakarta ANT Java/XML)
- Apache Commons Logging
- Apache SOAP (Simple Object Access Protocol)
- ICU (International Components for Unicode)
- J2SE™ platform 1.4.2_04 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Application Framework)
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding)
- JAXM (Java API for XML Messaging) Client Runtime

- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java APIs for XML-based Remote Procedure Call)
- JCAPI (Java Calendar API)
- JSS (Java Security Services)
- KT Search Engine
- LDAP C Language SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- Perl LDAP, incluido NSPERL
- SAAJ (SOAP with Attachments API for Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector
- XML C Library (libxml)

Java ES 2005Q1 (Versión 3)

Este apartado muestra el contenido de Java Enterprise System 2005Q1.

Componentes de la Versión 3 que se pueden seleccionar en el programa de instalación

En la página de selección de componentes del programa de instalación de Java ES, los componentes que se pueden elegir están agrupados según los servicios que proporcionan. La siguiente lista también muestra los componentes secundarios que se instalan con cada componente.

Communication & Collaboration Services

- Sun Java System Messaging Server 6 2005Q1
- Sun Java System Calendar Server 6 2005Q1
- Sun Java System Instant Messaging 7 2005Q1
 - Instant Messaging Server Core; incluye software para el servidor y multiplexor
 - Instant Messaging Resources
 - Access Manager Instant Messaging Service
- Sun Java System Portal Server 6 2005Q1
- Sun Java System Portal Server Secure Remote Access 6 2005Q1
 - Secure Remote Access Core
 - Puerta de enlace
 - Proxy Netlet
 - Proxy Rewriter
- Sun Java System Communications Express 2005Q1
- Herramienta de preparación de Sun Java System Directory

Web & Application Services

- Sun Java System Application Server Enterprise Edition 8.1 2005Q1
 - Domain Administration Server
 - Application Server Node Agent
 - Herramienta de administración de línea de comandos
 - Complemento de equilibrado de carga

Se puede utilizar con Web Server o Apache Web Server, seleccionándolo en el proceso de configuración. El valor predeterminado es Web Server.

 - PointBase
 - Aplicaciones de ejemplo
- Sun Java System Web Server 6 2005Q1 Update 1 Service Pack 4
- Sun Java System Message Queue 3 2005Q1

Directory & Identity Services

- Sun Java System Access Manager 6.3 2005Q1

Las herramientas de abastecimiento de Delegated Administrator para Portal Server y Messaging Server se instalan automáticamente con Access Manager.

 - Identity Management y Policy Services Core (incluye la utilidad Delegated Administrator)
 - Access Manager Administration Console
 - Common Domain Services for Federation Management
 - Access Manager SDK
- Sun Java System Directory Server 5 2005Q1
- Sun Java System Directory Proxy Server 5 2005Q1

Availability Services

- Sun Cluster 3.1 9/04
 - Sun Cluster Core
- Sun Cluster Agents for Sun Java System
 - HA/Scalable Sun Java System Web Server
 - HA Sun Java System Message Queue
 - HA Sun Java System Portal Server
 - HA Sun Java System Administration Server
 - HA Sun Java System Directory Server
 - HA Sun Java System Messaging Server
- HADB (se utiliza para almacenamiento de sesión de alta disponibilidad)

Administrative Services

- Sun Java System Administration Server 5 2005Q1
- SunSM Remote Services Net Connect 3.1.1

NOTA	Sun Cluster, Sun Cluster Agents y Sun Remote Services Net Connect no están disponibles en los sistemas operativos Solaris 10 ni Linux. Sun Remote Services Net Connect no está disponible en la plataforma Solaris x86.
-------------	--

Componentes compartidos de la Versión 3

Los componentes compartidos ofrecen servicios locales y compatibilidad tecnológica para los componentes seleccionables. Cuando se instalan componentes de Java ES, el programa de instalación instala automáticamente los componentes compartidos que se requieren, en caso de que no estén instalados.

Esta versión de Java ES incluye estos componentes compartidos:

- Ant (herramienta basada en Jakarta ANT Java/XML)
- Apache SOAP (Simple Object Access Protocol) Runtime
- Base de datos Berkeley
- Contenedor de agente común
- ICU (International Components for Unicode)
- J2SE™ (Java 2 Platform, Standard Edition) platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Web Application Framework)
- JavaHelp™ Runtime
- JavaMail™ Runtime
- JAXB (Java Architecture for XML Binding) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries) Runtime
- JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime
- JCAPAPI (Java Calendar API)
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- KTSE (KT Search Engine)
- LDAP C SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)

- Perl LDAP, incluido NSPERL
- SAAJ (SOAP with Attachments API for Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector (sólo para Solaris)
- Sun Java Monitoring Framework
- Sun Java Web Console
- Tomcat Servlet JSP Container
- XML C Library (libxml)
- WSCL (Web services Common Library)

Java ES 2005Q4 (Versión 4)

Este apartado muestra el contenido de Java Enterprise System 2005Q4

Componentes de la Versión 4 que se pueden seleccionar en el programa de instalación

En la página de selección de componentes del programa de instalación de Java ES, los componentes que se pueden elegir están agrupados según los servicios que proporcionan. La siguiente lista también muestra los componentes secundarios que se instalan con cada componente.

Communication & Collaboration Services

- Sun Java System Messaging Server 6.2 2005Q4
- Sun Java System Calendar Server 6.2 2005Q4
- Sun Java System Instant Messaging 7.0.1 2005Q4
 - Instant Messaging Server Core; incluye software para el servidor y multiplexor
 - Instant Messaging Resources
 - Access Manager Instant Messaging Service
- Sun Java System Portal Server 6.3.1 2005Q4
- Sun Java System Portal Server Secure Remote Access 6.3.1 2005Q4
 - Secure Remote Access Core
 - Puerta de enlace
 - Proxy Netlet
 - Proxy Rewriter
- Sun Java System Communications Express 6.2 2005Q4
- Herramienta de preparación de directorios de Sun Java System 6.3 2005Q4
- Sun Java System Communications Services Delegated Administrator 6.3 2005Q4
 - Delegated Administrator Console and Utility
 - Delegated Administrator Server

Web & Application Services

- Sun Java System Application Server Enterprise Edition 8.1 2005Q4

- Domain Administration Server
- Application Server Node Agent
- Herramienta de administración de línea de comandos
- Complemento de equilibrado de carga

Se puede utilizar con Web Server o Apache Web Server, seleccionándolo en el proceso de configuración. El valor predeterminado es Web Server.

- Base de datos PointBase
- Aplicaciones de ejemplo

- Sun Java System Web Server 6.1 Service Pack 5 2005Q4

- Sun Java Web Proxy Server 4.0.1 2005Q4

- Sun Java System Message Queue Enterprise Edition 3.6 SP3 2005Q4

- Sun Java Service Registry 3.0

Directory & Identity Services

- Sun Java System Access Manager 7.0 2005Q4

- Identity Management y Policy Services Core
- Access Manager Administration Console
- Common Domain Services for Federation Management
- Access Manager SDK

- Sun Java System Directory Server 5.2 2005Q4

- Sun Java System Directory Proxy Server 5.2 2005Q4

Availability Services

- Sun Cluster 3.1 8/05
 - Sun Cluster Core
 - Sun Cluster Agents for Sun Java System
 - HA Sun Java System Directory Server
 - HA Sun Java System Administration Server
 - HA/Scalable Sun Java System Web Server
 - HA Sun Java System Message Queue
 - HA Sun Java System Application Server
 - HA Sun Java System Messaging Server
 - HA Sun Java System Calendar Server
 - HA Sun Java System Instant Messaging
- Almacén de sesión de alta disponibilidad (HADB) 4.4.2

Administrative Services

- Sun Java System Administration Server 5.2 2005Q4

NOTA	Sun Cluster y Sun Cluster Agents son admitidos en el sistema operativo Solaris, pero no en el sistema operativo Linux.
-------------	--

Componentes compartidos de la Versión 4

Los componentes compartidos ofrecen servicios locales y compatibilidad tecnológica para los componentes seleccionables. Cuando se instalan componentes de Java ES, el programa de instalación instala automáticamente los componentes compartidos que se requieren, en caso de que no estén instalados.

Esta versión de Java ES incluye estos componentes compartidos:

- ANT (herramienta de creación basada en Jakarta ANT Java/XML)
- ACL (Apache Commons Logging)
- BDB (Base de datos Berkeley)
- CAC (Contenedor de agente común)
- Base de datos Derby
- ICU (International Components for Unicode)
- IM-SDK (Instant Messenger SDK)
- J2SE™ (Java 2 Platform, Standard Edition) platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Web Application Framework)
- JavaHelp™ Runtime
- JavaMail™ Runtime
- JAXB (Java Architecture for XML Binding) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries) Runtime
- JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime
- JCAPI (Java Calendar API)
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- KTSE (KT Search Engine)
- LDAP C SDK
- LDAP Java SDK

- MA (Mobile Access) Core
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP runtime with Attachments API for Java)
- SASL (Simple Authentication and Security Layer)
- SEDC (Sun Explorer Data Collector, sólo para Solaris)
- MFWK (Java ES Monitoring Framework)
- SJWC (Sun Java Web Console)
- WSCL (Web services Common Library)

Java ES 5 (Versión 5)

Este apartado muestra el contenido de Java Enterprise System 5.

Componentes de la Versión 5 que se pueden seleccionar en el programa de instalación

En la página de selección de componentes del programa de instalación de Java ES, los componentes que se pueden elegir están agrupados según los servicios que proporcionan. La siguiente lista también muestra los componentes secundarios que se instalan con cada componente. Tenga en cuenta que el programa de instalación de Java ES ya no admite los componentes de Communication Services.

Collaboration Services

- Sun Java System Portal Server 7.1
- Sun Java System Portal Server Secure Remote Access 7.1
 - Puerta de enlace
 - Proxy Netlet
 - Proxy Rewriter

Web & Application Services

- Sun Java System Application Server Enterprise Edition 8.2
 - Domain Administration Server
 - Application Server Node Agent
 - Herramienta de administración de línea de comandos
 - Complemento de equilibrado de carga

Se puede utilizar con Web Server o Apache Web Server, seleccionándolo en el proceso de configuración. El valor predeterminado es Web Server.

- Aplicaciones de ejemplo
- Sun Java System Web Server 7.0
 - Web Server 7.0 CLI
 - Web Server 7.0 Core
 - Web Server 7.0 Samples

- Sun Java Web Proxy Server 4.0.4
- Sun Java System Message Queue 3.7UR1
- Service Registry 3.1
 - Service Registry Client Support
 - Service Registry Deployment Support

Directory & Identity Services

- Sun Java System Access Manager 7.1
 - Identity Management y Policy Services Core
 - Access Manager Administration Console
 - Common Domain Services for Federation Management
 - Access Manager SDK
 - Autenticación distribuida
 - SDK de cliente
 - Cliente de recuperación ante fallo de sesión
- Sun Java System Directory Server Enterprise Edition 6
 - Java Enterprise System Directory Server 6 Core Server
 - Centro de control del servicio de directorio de Java Enterprise System
 - Utilidades de línea de comandos de Sun Java System Directory Server Enterprise Edition 6
 - Sun Java System Directory Proxy Server 6 Core Server

Availability Services

- Sun Cluster 3.1
 - Sun Cluster Core
- Sun Cluster Geographic Edition 3.1 2006Q4
- Sun Cluster Agents 3.1
 - HA Sun Java System Application Server
 - HA Sun Java System Message Queue
 - HA Sun Java System Directory Server

- HA Sun Java System Messaging Server
- HA Sun Java System Application Server EE (HADB)
- HA/Scalable Sun Java System Web Server
- HA Instant Messaging
- HA Sun Java System Calendar Server
- ...
- Almacén de sesión de alta disponibilidad de Sun Java System 4.4.3

Servicios compartidos

- Todos los componentes compartidos
Consulte [“Componentes compartidos de la Versión 5”](#) en la página 472.
- Consola de supervisión de Sun Java System 1.0
- Java DB
 - Cliente de Java DB
 - Java DB Server

NOTA	Sun Cluster y Sun Cluster Agents son admitidos en el sistema operativo Solaris, pero no en el sistema operativo Linux.
-------------	--

Componentes compartidos de la Versión 5

Los componentes compartidos ofrecen servicios locales y compatibilidad tecnológica para los componentes seleccionables. Cuando se instalan componentes de Java ES, el programa de instalación instala automáticamente los componentes compartidos que se requieren, en caso de que no estén instalados.

Esta versión de Java ES incluye estos componentes compartidos:

- ANT (herramienta de creación basada en Jakarta ANT Java/XML)
- ACL (Apache Commons Logging)
- BDB (Base de datos Berkeley)
- CAC (Contenedor de agente común) sólo para Sun Cluster
- CAC (Contenedor de agente común)
- FIS (FastInfoSet)
- ICU (International Components for Unicode)
- IM-SDK (Instant Messenger SDK)
- J2SE™ (Java 2 Platform, Standard Edition) platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Web Application Framework)
- JavaHelp™ Runtime
- JavaMail™ Runtime
- JAXB (Java Architecture for XML Binding) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries) Runtime
- JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime
- JAXWS (Java API for Web Services) Runtime
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- JSTL (JSP Standard Library Template)
- KTSE (KT Search Engine)

- LDAP C SDK
- LDAP Java SDK
- MA (Mobile Access) Core
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP runtime with Attachments API for Java)
- SASL (Simple Authentication and Security Layer)
- SEDC (Sun Explorer Data Collector, sólo para Solaris)
- MFWK (Java ES Monitoring Framework)
- SJWC (Sun Java Web Console)
- WSCL (Web services Common Library)
- XWSS (XML Web Services Security)

A

- Access Manager
 - abreviatura 30
 - componentes secundarios 465, 470
 - dependencias con componentes compartidos 49
 - dependencias de los componentes de productos 53
 - enfoque de actualización 36
- AccessManagerConfig-base path* 282
- Almacén de sesión de alta disponibilidad (HADB)
 - abreviatura 31
 - dependencias con componentes compartidos 49
 - dependencias de los componentes de productos 54
 - enfoque de actualización 37
- Ant (herramienta basada en Jakarta ANT Java/XML)
 - Consulte* ANT
- Apache Commons Logging, *consulte* ACL
- Application Server
 - abreviatura 30
 - componentes secundarios 465, 469
 - configuración post-instalación 241
 - dependencias con componentes compartidos 49
 - dependencias de los componentes de productos 54
 - enfoque de actualización 36
- archivos JSP, personalizados 285, 294, 300, 328

B

- Base de datos Berkeley, *consulte* BDB

C

- Componente compartido ACL
 - en la tabla de dependencias 49
 - nombre completo 31
- Componente compartido ANT
 - en la tabla de dependencias 49
 - nombre completo 31
- Componente compartido BDB
 - en la tabla de dependencias 49
 - nombre completo 31
- Componente compartido CAC
 - en la tabla de dependencias 49
 - nombre completo 31
- Componente compartido de la base de datos Derby 467
- Componente compartido FIS
 - en la tabla de dependencias 49
 - nombre completo 31
- Componente compartido ICU
 - en la tabla de dependencias 49
 - nombre completo 32
- Componente compartido IM-SDK
 - en la tabla de dependencias 49
 - nombre completo 32
- Componente compartido JAF
 - en la tabla de dependencias 49

- nombre completo [32](#)
- Componente compartido JATO
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido Java SE
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JAXB
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JAXP
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JAXR
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JAX-RPC
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JAXWS
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JCAPI
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JHELP
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JMAIL
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JMDK
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JSS
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido JSTL
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido KTSE
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido LDAP C Language SDK [473](#)
- Componente compartido LDAP C SDK
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido LDAP J SDK [473](#)
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido MA Core
 - en la tabla de dependencias [49](#)
 - nombre completo [32](#)
- Componente compartido MFWK
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido NSPR
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido NSS
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido SAAJ
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido SASL
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido SEDC
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido SJWC
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido WSCL
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- Componente compartido XWSS
 - en la tabla de dependencias [50](#)
 - nombre completo [32](#)
- componentes compartidos
 - componentes de productos dependientes [48](#)
 - interdependencias [51](#)
 - Java ES 2003Q4 (Versión 1) [455](#)
 - Java ES 2004Q2 (Versión 2) [457](#)
 - Java ES 2005Q1 (Versión 3) [462](#)
 - Java ES 2005Q4 (Versión 4) [467](#)
 - Java ES 5 (Versión 5) [472](#)
- componentes de productos

- dependencia con componentes compartidos 48
- interdependencias 53
- Java ES 2003Q4 (Versión 1) 454
- Java ES 2004Q2 (Versión 2) 456
- Java ES 2005Q1 (Versión 3) 459
- Java ES 2005Q4 (Versión 4) 464
- Java ES 5 (Versión 5) 469

Contenedor de agente común, *consulte* CAC

convenciones

- símbolo 23

- tipográficas 23

convenciones de símbolos 23

convenciones tipográficas 23

D

dependencias

- componente de producto, con los componentes compartidos 48

- entre componentes compartidos 51

- entre componentes de productos 53

Directory Proxy Server

- abreviatura 30

- dependencias con componentes compartidos 49

- dependencias de los componentes de productos 54

- enfoque de actualización 36

Directory Server

- abreviatura 31

- dependencias con componentes compartidos 49

- dependencias de los componentes de productos 54

- enfoque de actualización 36

DirServer-base path (Directory Server 6.0) 108, 126

F

FastInfoSet, *consulte* FIS

H

HADB-base path 180

I

Instant Messenger SDK, *consulte* IM-SDK

International Components for Unicode, *consulte* ICU

J

Java 2 Platform, Standard Edition, *Consulte* J2SE

Java 2 Platform, Standard Edition, *consulte* Java SE

Java API for XML Processing, *Consulte* JAXP

Java API for XML Registries, *Consulte* JAXR

Java API for XML-based Remote Procedure Call, *consulte* JAX-RPC

Java Architecture for XML Binding, *consulte* JAXB

Java Calendar API, *consulte* JCAPI

Java DB

- abreviatura 31

- dependencias con componentes compartidos 49

- dependencias de los componentes de productos 54

- enfoque de actualización 37

Java Dynamic Management Kit, *consulte* JDMK

Java ES 2003Q4 (Versión 1)

- componentes compartidos 455

- componentes de productos 454

Java ES 2004Q2 (Versión 2)

- componentes compartidos 457

- componentes de productos 456

Java ES 2005Q1 (Versión 3)

- componentes compartidos 462

- componentes de productos 459

Java ES 2005Q4 (Versión 4)

- componentes compartidos 467

- componentes de productos 464

Java ES 5 (Versión 5)

- componentes compartidos 472

- componentes de productos 469

Java ES Monitoring Framework, *consulte* MFWK
 Java Security Services, *consulte* JSS
 Java Studio Web Application Framework, *consulte* JATO
 JAVA_HOME [383](#), [395](#), [398](#), [425](#), [428](#), [447](#), [449](#)
 JavaBeans Activation Framework, *Consulte* JAF
 JavaHelp, *consulte* JHELP
 JavaMail, *Consulte* JMAIL
 JSP Standard Library Template, *consulte* JSTL

K

KT Search Engine, *Consulte* KTSE

M

Message Queue
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de
 productos [55](#)
 enfoque de actualización [37](#)
MessageQueue-base path [193](#)
 Mobile Access Core, *consulte* MA core
 Monitoring Console
 abreviatura [31](#)

N

Netscape Portable Runtime, *Consulte* NSPR
 Network Security Services, *consulte* NSS

P

Portal Server
 abreviatura [31](#)

dependencias con componentes compartidos [49](#)
 dependencias de los componentes de
 productos [55](#)
 enfoque de actualización [37](#)
 Portal Server Secure Remote Access
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de
 productos [56](#)
 enfoque de actualización [37](#)

R

RegistryDomainR4-base path [249](#)
RegistryDomainR5-base path [250](#)
rel4CAC-base-dir path [78](#)
rel5CAC-admin-dir path [78](#)
 Ruta de *AccessManager-base* [282](#)
 ruta de *AppServer7-base* [220](#)
 ruta de *AppServer7Config-base* [220](#)
 ruta de *AppServer8-base* [220](#)
 ruta de *AppServer8Config-base* [220](#)
 ruta de *AppServer8Install-base* [220](#)
 Ruta de *PortalServer6-base* [338](#), [412](#)
 Ruta de *PortalServer6Config-base* [338](#), [412](#)
 Ruta de *PortalServer7-base* [338](#), [412](#)
 Ruta de *PortalServer7Config-base* [338](#), [412](#)
 Ruta de *PortalServer7Data-base* [338](#), [412](#)
 Ruta de *SunClusterGeo-base* [95](#)
 Ruta de *WebServer6-base* [141](#)
 Ruta de *WebServer7-base* [142](#)
 Ruta de *WebServer7Config-base* [142](#)

S

SAML [308](#), [334](#)
 secuencia de comandos amconfig (Access Manager) [300](#)
 secuencia de comandos ampre71upgrade (Access Manager) [297](#), [326](#)

secuencia de comandos amupgrade (Access Manager) [305, 332](#)
 secuencia de comandos mqupgrade (Message Queue) [213, 215](#)
 secuencia de comandos postInstall (Application Server) [241](#)
 secuencias de comandos
 amconfig (Access Manager) [300](#)
 ampre71upgrade (Access Manager) [297, 326](#)
 amupgrade (Access Manager) [305, 332](#)
 mqmigrate (Message Queue) [215](#)
 mqupgrade (Message Queue) [213](#)
 postInstall (Application Server) [241](#)
 Security Assertion Markup Language, *consulte* SAML
serverRoot path (Directory Server 5.x) [108, 126](#)
 Service Registry
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de productos [56](#)
 enfoque de actualización [37](#)
ServiceRegistryR4-base path [171, 249](#)
ServiceRegistryR5-base path [250](#)
 Simple Authentication and Security Layer, *Consulte* SASL
 SML Web Services Security, *consulte* XWSS
 SOAP runtime with Attachments API for Java, *consulte* SAAJ
 Sun Cluster
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de productos [57](#)
 enfoque de actualización [37](#)
 Sun Cluster Geographic Edition
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de productos [57](#)
 enfoque de actualización [37](#)
 Sun Explorer Data Collector, *consulte* SEDC
 Sun Java Web Console, *consulte* SJWC

U

utilidad db2bak [293](#)

V

Variable de entorno ANT_HOME [357, 360, 383, 395, 398, 425, 428, 447, 449](#)

Variable de entorno JAVA_HOME [302, 330, 357, 360](#)

W

Web Proxy Server
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de productos [57](#)
 enfoque de actualización [37](#)
 Web Server
 abreviatura [31](#)
 dependencias con componentes compartidos [49](#)
 dependencias de los componentes de productos [57](#)
 enfoque de actualización [37](#)
 Web services Common Library, *consulte* WSCL
WebProxyServer-base path [263](#)

Index of Fonts

Courier @ 10.0 pt 23–28, 30, 35–36, 46, 61–62, 64–66, 72, 75, 77–79, 82–83, 86–87, 89–93, 100–101, 103–105, 109, 112, 115–122, 130, 135–138, 142, 147–153, 155–156, 159–166, 175–178, 185–190, 196, 199–200, 202–205, 207–216, 220, 228, 230–232, 235, 237, 239–245, 255, 257–262, 268, 270–273, 275–276, 278, 282, 287, 289–290, 292–302, 304–308, 310–311, 313, 318–319, 321–334, 339, 342, 345–346, 349, 351, 353–376, 378–409, 413, 415, 418, 420–432, 434–438, 442–444, 446–450, 463

Courier @ 7.0 pt 134, 195, 222, 349, 352, 421

Courier @ 7.5 pt 2

Courier @ 8.25 pt 23–26, 36–37, 42–43, 76–78, 83–84, 89, 95, 108, 110, 126, 128, 141–142, 144–145, 153–158, 161, 171, 180, 182, 193, 195–196, 220, 222–224, 249–250, 252, 256, 263, 265, 268, 271–272, 275, 282, 284–285, 296–298, 301–306, 325–326, 330–331, 333, 338, 340–341, 349, 351–352, 354, 412, 415, 421

Courier @ 9.0 pt 18–20, 100, 115–116, 118–120, 133–134, 153, 156, 158, 161, 163, 165, 175, 201, 211, 229, 256, 292, 301–302, 304–305, 330, 333, 351

Courier @ 9.5 pt 23–24, 77–79, 100, 115–116, 122, 133, 147, 216, 401

Helvetica @ 10.0 pt 44, 58, 63, 77, 83, 90, 95, 101, 104, 107–108, 121–122, 125–126, 141, 171, 179, 193, 219–220, 224, 226, 238, 241–242, 249, 263, 271, 281–282, 294, 309, 315–316, 329, 334, 337, 343, 346, 350, 353, 357–359, 361, 373, 378, 381, 384–385, 396, 399, 412, 427, 438, 447, 455, 461, 466, 471

Helvetica @ 11.0 pt 34–35, 89–91, 100–102, 115–117, 133–135, 147–148, 151, 163–166, 175–176, 185–187, 200–202, 211–212, 228–230, 237, 239, 244–245, 255–257, 260, 268–271, 273, 275–276, 292–296, 308, 324–325, 349, 351, 353–356, 359, 363–364, 366–367, 370, 393, 396, 400–404, 406–407, 420–425, 427, 429–431, 445, 447, 450

Helvetica @ 12.0 pt 34, 36, 46–48, 63–64, 66, 77, 85, 87, 91–93, 97–99, 102, 105, 112, 115–116, 121–123, 130–131, 133–134, 137–138, 144–145, 147–148, 162–163, 166, 173, 175–178, 185–186, 189–191, 197, 200, 202–204, 208–212, 214, 216–217, 225, 228, 230, 232–233, 236, 239, 244–245, 252–253, 255, 257,

260–261, 266, 268–269, 271–273, 275–276, 278–279, 286–288, 291, 295, 306–308, 312–314, 321, 323, 334–335, 342–344, 349, 355, 359, 362–363, 370, 372, 378, 381–382, 386, 390, 393, 396, 399–400, 407, 409, 415–417, 420, 424, 427, 429, 431, 433, 441–443, 445, 447, 449–450

Helvetica @ 14.0 pt 29, 69, 81, 95, 107, 125, 141, 171, 179, 193, 219, 249, 263, 281, 337, 411, 453

Helvetica @ 15.0 pt 475, 477–479

Helvetica @ 16.0 pt 1

Helvetica @ 17.0 pt 22–26, 30–31, 33, 38, 40–41, 44–46, 48, 52, 61–62, 65–66, 70, 72–73, 76, 78, 82–87, 96–99, 109, 111–112, 114–115, 122, 127, 129, 132–133, 138, 142–144, 146–147, 172–174, 178, 181–185, 194–197, 199–200, 205, 207–208, 210, 221, 224–225, 227–228, 235–236, 251–252, 254–255, 262, 264–265, 267–268, 274–275, 282–283, 285–286, 290–291, 309, 311, 315, 320, 323, 335, 339–341, 346, 348, 372, 377–381, 386, 390–392, 409, 413–415, 418, 420, 433, 439–445, 451, 454–457, 459, 462, 464, 467, 469, 472

Helvetica @ 20.0 pt 22, 24, 27–28, 30, 33, 38, 40, 48, 57, 61–62, 70, 75, 82, 86, 96, 98, 109, 114, 123, 127, 132, 139–140, 142, 146, 168–169, 172, 174, 181, 184, 192, 194, 199, 206–207, 221, 227, 234–235, 246, 251, 254, 264, 267, 274, 282, 290, 315, 320, 339, 346, 377, 380, 391, 413, 418, 439, 441, 444, 454, 456, 459, 464, 469

Helvetica @ 22.0 pt 1, 5, 17, 21, 29, 69, 81, 95–96, 107, 125, 127, 141, 171–172, 179, 193, 219, 249, 251, 263, 281, 337, 411, 453, 475, 1, 1, 1, 3, 7, 17, 19, 49

Helvetica @ 7.0 pt 5–56

Helvetica @ 8.0 pt 1

Helvetica @ 8.25 pt 23–26, 30–32, 36–37, 39, 42–43, 45, 49–51, 53–57, 61, 76–78, 83–84, 89, 95–97, 100, 108–111, 115–116, 126, 128–129, 133–134, 141, 143–145, 147, 153–159, 161–163, 165, 171–173, 175, 180–182, 185–187, 193, 195–196, 201, 211, 220, 222–224, 229, 249, 251–252, 256, 263–265, 268–271, 275, 282–286, 288, 292, 296–298, 301–306, 309, 316, 325–326, 330–331, 333, 338, 340–341, 344–345, 349, 351–352, 354, 374, 391, 412, 414–415, 421, 434, 444

Helvetica @ 9.0 pt 1, 5–16, 23–25, 30–31, 36, 39, 42, 45, 47, 49, 51, 53, 58–61, 75–79, 83–84, 89, 91–92, 95–97, 100–105, 108–109, 111, 115, 117–120, 122, 126, 128–129, 133–137, 141, 143–145, 147, 151–153, 155–156, 158–167, 171–173, 175–177, 180–182, 185, 187–190, 193, 195–196, 201–205, 211–216, 220, 222–224, 229–232, 237–243, 247–249, 251–252, 256–265, 268–273, 275–278, 282–283, 285, 288, 292–293, 295–302, 304–311, 313, 316, 318–319, 321–334, 338, 340, 344, 349–351, 354–362, 364–367, 370–372, 374–391, 393–409, 412, 414–415, 421–423, 425–432, 434–439, 442–444, 446–450, 466

Palatino @ 10.0 pt 21–31, 33–36, 38–42, 44–48, 50–53, 57–67, 69–93, 95–105, 107–109, 111–127, 129–153, 155–156, 159–169, 171–179, 181–217, 219–221, 224–279, 281–283, 285–302, 304–335, 337, 339–351, 353–367, 370–451, 453–473, 1–3, 1, 3–5, 7–17, 19–47, 49–55

Palatino @ 6.0 pt 23–25, 30–31, 36, 39, 42, 44–45, 49, 53, 58, 61, 63, 76–78, 83–84, 89–90, 95–97, 100–101, 104, 107–109, 111, 115, 119–122, 125–126, 128–129, 133, 141, 143–145, 147, 153, 156, 158, 161, 163, 165, 171–173, 175, 179–182, 185, 187, 193, 195–196, 201, 211, 219–220, 222–224, 226, 229,

238, 241–242, 249, 251–252, 256, 263–265, 268–269, 271, 275, 281–283, 285, 288, 292, 294, 296–297, 301–302, 304–305, 309, 315–316, 325–326, 329–330, 333–334, 337–338, 340, 343–344, 346, 349–351, 353–354, 357–359, 361, 373, 378, 381, 384–385, 391, 396, 399, 412, 414–415, 421, 427, 438, 444, 447, 455, 461, 466, 471

Palatino @ 7.0 pt 50, 57, 61, 84, 89, 134, 144, 195, 222–223, 270–271, 296, 298, 303, 306, 325–326, 331, 333, 349, 352, 391, 421, 444

Palatino @ 7.5 pt 2–3

Palatino @ 8.0 pt 2

Palatino @ 8.25 pt 24–26, 42–43, 78, 108, 110, 126, 128, 141–142, 144–145, 156, 158–159, 161, 171, 173, 180, 193, 195–196, 220, 222, 224, 252, 263, 265, 271, 282, 284–285, 288, 297–298, 301–305, 326, 330–331, 333, 338, 340–341, 344–345, 351–352, 354, 398, 412, 415, 448

Palatino @ 9.0 pt 5–20, 23–25, 30–31, 36, 39, 42, 49, 51, 53, 61, 76–78, 83–84, 89, 95–97, 100, 108–109, 111, 115, 119–120, 126, 128–129, 133, 141, 143–145, 147, 153, 156, 158, 161, 163, 165, 171–173, 175, 180–182, 185, 187, 193, 195–196, 201, 211, 220, 222–224, 229, 249, 251–252, 256, 263–265, 268–269, 271, 275, 282–283, 285, 288, 292, 296–297, 301–302, 304–305, 309, 316, 325–326, 330, 333, 338, 340, 344, 349, 351, 354, 374, 391, 412, 414–415, 421, 434, 444, 475–479

Palatino @ 9.5 pt 77–79, 115, 122, 133, 147, 401

ZapfDingbats @ 5.0 pt 30, 65, 148–151, 159, 184, 242, 293–294, 300, 305, 307, 313, 328–329, 332, 348, 355, 383, 392, 419, 424, 426, 428, 430, 459–461, 464–466, 469–471

List of Conditional Text

List of Marker Text for Alternative Text

ImageAltText:	Figura 1-1	Diagrama que muestra relaciones de dependencia entre componentes compartidos. Éstas se dividen en dos grupos: los relacionados con las interdependencias de JAX, y los utilizados para la visualización o seguridad, que a menudo dependen de J2SE o NSPR. 51
ImageLongDescByRef:	Figura 1-1	longdesc-fig1-1.html 51
ImageAltText:	Figura 14-1	Diagrama que muestra la arquitectura de implementación de varias instancias de Access Manager. 309
ImageAltText:	Figura 14-2	Diagrama que muestra la arquitectura de implementación de varias instancias de Access Manager. 316
ImageAltText:	Figura 15-1	Diagrama que muestra la arquitectura de implementación de ejemplo de varias instancias de Portal Server que acceden a varias instancias de Access Manager. 374
ImageAltText:	Figura 16-1	Diagrama que muestra la arquitectura de implementación de ejemplo de varias instancias de la puerta de enlace que acceden a varias instancias de Portal Server que, a su vez, acceden a varias instancias de Access Manager. 434

List of Table Summaries Marker Text

TableSummary:	Tabla 1	Convenciones de tipo de letra utilizadas en este libro.	23
TableSummary:	Tabla 2	Convenciones de símbolos utilizadas en este libro.	23
TableSummary:	Tabla 3	Convenciones de indicadores de intérprete de comandos utilizadas en esta guía.	24
TableSummaryNotReq:	Tabla 4	Documentación	25
TableSummary:	Tabla 1-8	Dependencias de los productos componentes	53
TableSummary:	Tabla 3-1	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1.	83
TableSummary:	Tabla 4-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1.	96
TableSummary:	Tabla 5-2	Esta tabla muestra la guía de actualización de Directory Server 2006Q3.	109
TableSummary:	Tabla 6-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1.	128
TableSummary:	Tabla 7-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1.	143
TableSummary:	Tabla 8-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1.	172
TableSummary:	Tabla 9-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1.	181

TableSummary:	Tabla 10-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 195
TableSummaryNotReq:	Tabla 10-3	196
TableSummary:	Tabla 11-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 222
TableSummary:	Tabla 11-3	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 223
TableSummary:	Tabla 12-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 251
TableSummary:	Tabla 13-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 264
TableSummary:	Tabla 13-5	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 269
TableSummary:	Tabla 13-6	Esta tabla muestra las revisiones necesarias para actualizar Administration Server en Linux. 271
TableSummary:	Tabla 14-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 283
TableSummary:	Tabla 14-4	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 288
TableSummary:	Tabla 14-6	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 296
TableSummary:	Tabla 14-13	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 325
TableSummary:	Tabla 15-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 340
TableSummary:	Tabla 15-4	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 344
TableSummary:	Tabla 15-8	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 391

TableSummary:	Tabla 16-2	Esta tabla muestra el proceso de actualización de Access Manager 2005Q1. 414
TableSummary:	Tabla 16-5	Esta tabla muestra las revisiones necesarias para actualizar Administration Server, Directory Server y Directory Proxy Server en Solaris. 444

List of Markers That Insert URLs and Links in HTML Output Files

Starts Link Type13: <http://www.sun.com/patents> 2

Ends Link Type14: , 2

Starts Link Type13: <http://www.sun.com/patents> 2

Ends Link Type14: et 2

Starts Link Type13: <http://docs.sun.com> 24

Ends Link Type14: SM 24

Starts Link Type13: <http://docs.sun.com> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/coll/1286.2> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/819-4893> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/820-0167> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/819-2326> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/819-5079> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/819-4891> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/819-4892> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/819-6553> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/819-5081> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/819-3875> 26

Ends Link Type14: 26

Starts Link Type13: java.sun.com 27

Ends Link Type14: , 27

Starts Link Type13: www.sun.com 27

Ends Link Type14: , 27

Starts Link Type13: developers.sun.com 27

Ends Link Type14:) 27

Starts Link Type13: <http://www.sun.com/software/download/> 27

Ends Link Type14: 27

Starts Link Type13: <http://www.sun.com/service/sunjavasystem/sjsserviceessuite.html> 27

Ends Link Type14: 27

Starts Link Type13: <http://sunsolve.sun.com/> 27

Ends Link Type14: 27

Starts Link Type13: <http://developers.sun.com/prodtech/index.html> 27
Ends Link Type14: 27

Starts Link Type13: <http://www.sun.com/software/javaenterprisesystem/index.html> 27
Ends Link Type14: 27

Starts Link Type13: <http://www.sun.com/service/contacting> 27
Ends Link Type14: . 27

Starts Link Type13: <http://docs.sun.com> 28
Ends Link Type14: y 28

Starts Link Type13: <http://docs.sun.com/doc/819-2330> 30
Ends Link Type14: : 30

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
35
Ends Link Type14: 35

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
36
Ends Link Type14: 36

Starts Link Type13: <http://docs.sun.com/doc/819-4893> 42
Ends Link Type14: . 42

Starts Link Type13: <http://docs.sun.com/doc/819-4893> 42
Ends Link Type14: . 42

Starts Link Type13: <http://docs.sun.com/doc/819-0062> 43
Ends Link Type14: , 43

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
46
Ends Link Type14: 46

Starts Link Type13: <https://www.redhat.com/apps/download/> 46

Ends Link Type14: . 46

Starts Link Type13: <http://docs.sun.com/doc/819-5079> 62

Ends Link Type14: . 62

Starts Link Type13: <http://docs.sun.com/doc/819-5079> 64

Ends Link Type14: . 64

Starts Link Type13: <http://docs.sun.com/doc/819-5079> 65

Ends Link Type14: . 65

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 78

Ends Link Type14: . 78

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 78

Ends Link Type14: . 78

Starts Link Type13: <http://docs.sun.com/doc/819-1405/6n3p13hac?a=view> 82

Ends Link Type14:) 82

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 82

Ends Link Type14: . 82

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 87

Ends Link Type14: . 87

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 87

Ends Link Type14: . 87

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 90

Ends Link Type14: . 90

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 90

Ends Link Type14: . 90

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 91

Ends Link Type14: . 91

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 91
Ends Link Type14: . 91

Starts Link Type13: <http://docs.sun.com/doc/816-3381/6m9lratq9?a=view#gcpom> 92
Ends Link Type14: . 92

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnrc?a=view> 93
Ends Link Type14: . 93

Starts Link Type13: <http://docs.sun.com/doc/817-7501> 103
Ends Link Type14: . 103

Starts Link Type13: <http://docs.sun.com/doc/817-7500> 103
Ends Link Type14: . 103

Starts Link Type13: <http://docs.sun.com/doc/817-7500> 104
Ends Link Type14: . 104

Starts Link Type13: <http://docs.sun.com/doc/817-7501> 104
Ends Link Type14: . 104

Starts Link Type13: <http://docs.sun.com/doc/819-0991> 109
Ends Link Type14: . 109

Starts Link Type13: <http://docs.sun.com/doc/819-0062> 110
Ends Link Type14: . 110

Starts Link Type13: <http://docs.sun.com/doc/819-0062> 110
Ends Link Type14: . 110

Starts Link Type13: <http://docs.sun.com/doc/819-0994> 112
Ends Link Type14: . 112

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 120
Ends Link Type14: . 120

Starts Link Type13: <http://docs.sun.com/doc/819-0994> 121

Ends Link	Type14:	.	121
Starts Link	Type13:	http://docs.sun.com/doc/819-0062	128
Ends Link	Type14:	.	128
Starts Link	Type13:	http://docs.sun.com/doc/819-0062	128
Ends Link	Type14:	.	128
Starts Link	Type13:	http://docs.sun.com/doc/819-0994	130
Ends Link	Type14:	.	130
Starts Link	Type13:	http://docs.sun.com/doc/819-0995	137
Ends Link	Type14:		137
Starts Link	Type13:	http://docs.sun.com/doc/819-0994	137
Ends Link	Type14:	.	137
Starts Link	Type13:	http://docs.sun.com/doc/819-2629	142
Ends Link	Type14:	.	142
Starts Link	Type13:	http://docs.sun.com/doc/819-2625	151
Ends Link	Type14:	.	151
Starts Link	Type13:	http://docs.sun.com/doc/819-3283	156
Ends Link	Type14:	.	156
Starts Link	Type13:	http://docs.sun.com/doc/819-4740/6n4r9qo7n?a=view	187
Ends Link	Type14:		187
Starts Link	Type13:	http://docs.sun.com/819-4467/6n6k98brl?a=view	196
Ends Link	Type14:	.	196
Starts Link	Type13:	http://docs.sun.com/doc/819-4467	203
Ends Link	Type14:	.	203
Starts Link	Type13:	http://docs.sun.com/doc/819-4467	209
Ends Link	Type14:	para	209

Starts Link Type13: <http://docs.sun.com/doc/819-4467> 210
Ends Link Type14: para 210

Starts Link Type13: <http://docs.sun.com/doc/819-4467> 212
Ends Link Type14: . 212

Starts Link Type13: <http://docs.sun.com/doc/819-4467> 216
Ends Link Type14:) 216

Starts Link Type13: <http://docs.sun.com/doc/819-4736> 220
Ends Link Type14: . 220

Starts Link Type13: <http://docs.sun.com/doc/819-0062> 222
Ends Link Type14: . 222

Starts Link Type13: <http://docs.sun.com/doc/819-4733> 242
Ends Link Type14: . 242

Starts Link Type13: <http://docs.sun.com/doc/819-4740> 242
Ends Link Type14: . 242

Starts Link Type13: <http://docs.sun.com/doc/819-4736> 243
Ends Link Type14: y 243

Starts Link Type13: <http://docs.sun.com/doc/819-4737/6n6sao3ju?a=view> 243
Ends Link Type14: . 243

Starts Link Type13: <http://docs.sun.com/doc/819-4737> 245
Ends Link Type14: . 245

Starts Link Type13: <http://docs.sun.com/doc/817-4640> 257
Ends Link Type14: . 257

Starts Link Type13: <http://docs.sun.com/doc/817-4640> 258
Ends Link Type14: . 258

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> 270

Ends Link Type14: 270

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> 272

Ends Link Type14: 272

Starts Link Type13: <http://docs.sun.com/doc/819-5492> 278

Ends Link Type14:) 278

Starts Link Type13: <http://docs.sun.com/doc/819-5494> 278

Ends Link Type14:) 278

Starts Link Type13: <http://docs.sun.com/doc/819-4683> 282

Ends Link Type14: . 282

Starts Link Type13: <http://docs.sun.com/doc/819-0062> 284

Ends Link Type14: . 284

Starts Link Type13: <http://docs.sun.com/doc/819-4683> 287

Ends Link Type14:) 287

Starts Link Type13: <http://docs.sun.com/doc/8197-0995> 293

Ends Link Type14: . 293

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> 296

Ends Link Type14: 296

Starts Link Type13: <http://docs.sun.com/doc/819-4675> 300

Ends Link Type14: . 300

Starts Link Type13: <http://docs.sun.com/doc/819-4670> 300

Ends Link Type14: . 300

Starts Link Type13: <http://docs.sun.com/doc/819-4670> 308

Ends Link Type14:) 308

Starts Link Type13: <http://docs.sun.com/doc/819-7561> 321

Ends Link Type14:) 321

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
325

Ends Link Type14: 325

Starts Link Type13: <http://docs.sun.com/doc/819-4675> 328

Ends Link Type14: . 328

Starts Link Type13: <http://docs.sun.com/doc/819-4670> 334

Ends Link Type14:) 334

Starts Link Type13: <http://docs.sun.com/doc/819-4986/6n4l3f365?a=view> 339

Ends Link Type14: . 339

Starts Link Type13: <http://docs.sun.com/doc/819-5030> 342

Ends Link Type14: . 342

Starts Link Type13: <http://docs.sun.com/doc/819-7561> 351

Ends Link Type14: . 351

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 370

Ends Link Type14: . 370

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
394

Ends Link Type14: 394

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
397

Ends Link Type14: 397

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 407

Ends Link Type14: . 407

Starts Link Type13: <http://docs.sun.com/doc/819-4986/6n4l3f365?a=view> 413

Ends Link Type14: . 413

Starts Link Type13: <http://docs.sun.com/doc/819-5030> 415

Ends Link Type14: . 415

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 431

Ends Link Type14: . 431

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
446

Ends Link Type14: 446

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
448

Ends Link Type14: 448

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 450

Ends Link Type14: . 450

List of Imported Graphics

Dir &

Filename ../../070412_UpgradeGuide_for_UNIX/Es/Final/
SJESUMG/820-0895/frame-src/figures/sharedCompDependenc
ies.eps 51

Dir &

Filename ../../070412_UpgradeGuide_for_UNIX/Es/Final/
SJESUMG/820-0895/frame-src/figures/redundacyArch-AM.eps
309

Dir &

Filename ../../070412_UpgradeGuide_for_UNIX/Es/Final/
SJESUMG/820-0895/frame-src/figures/redundacyArch-AM.eps
316

Dir &

Filename ../../070412_UpgradeGuide_for_UNIX/Es/Final/
SJESUMG/820-0895/frame-src/figures/redundacyArch-PS.eps
374

Dir &

Filename ../../070412_UpgradeGuide_for_UNIX/Es/Final/
SJESUMG/820-0895/frame-src/figures/redundacyArch-PS-SRA
.eps. 434

List of Markers

12326: Head1: Who Should Use This Book 22
48092: Head1: Conventions Used in This Book 22
18195: Head1: Related Documentation 24
20210: TableCaptionP: Sun ONE Application Server documentation roadmap 25
39375: Head1: Accessing Sun Resources Online 27
60891: Head1: Contacting Sun Technical Support 27
94390: Head1: Related Third-Party Web Site References 27
18048: Head1: Sun Welcomes Your Comments 28
84055: ChapNumber: Chapter 8 29
75725: ChapTitle: Planning for Upgrades 29
64237: Head1: Java ES 5 Components 30
94762: TableCaption: Table 1-1 Java ES Release 4 Product Components 30
57330: Head2: Release 4 Shared Components 31
32712: TableCaption: Table 1-2 Java ES Release 4 Shared Components 31
53515: Head1: Upgrade Planning 33
19005: Head3: Using the Upgrade Option of the Java ES Release 5 Installer 34
26271: Head3: Performing a Fresh Install of the Component 35
28798: Head3: Running a Component-specific Upgrade Script 35
97158: Head3: Patching Existing Component Packages 35

47583: Head2: Shared Component Upgrades	38
95877: Head1: The Upgrade Process	38
87930: Head1: Upgrade Planning	40
96243: Head2: Upgrade Dependencies	40
96632: Head2: Upgrade Paths	41
23983: TableCaptionWide: Table 1-4 Upgrade Paths to Java ES 2005Q4 (Release 4)	42
48275: Head2: Selective Upgrade or Upgrade All	44
77667: Head4: Component Redundancy	45
99494: Head2: Operating System Issues	46
55223: Head3: Required Operating System Patches	46
65555: Head3: Dual Upgrades: Java ES and Operating System Software	46
40351: Step1: 1. Backing up all Java ES configuration files and customizations.	47
49654: Head1: Java ES Component Dependencies	48
83054: Head2: Dependencies on Shared Components	48
86783: TableCaption: Table 1-2 Shared Component Dependencies of Product Componets	49
80863: FigureCaption: Figure 1-1 Shared Component Inter-dependencies	51
17819: Head3: Infrastructure Dependencies	52
26535: TableCaption: Table 1-3 Java ES Product Component Dependencies	53
53904: Head1: Preparing for Upgrades	57
88510: Head1: Special Cases	61
13934: TableCaptionIndent: Table 6-3 Patches to Upgrade Messaging Server on Solaris	61
22989: Head1: Java ES Release 5 and Solaris 10 Zones	62
14735: Head2: Zone Support in the Java ES Release 5 Installer	62
64070: Head2: Recommended Upgrade Practices	65
20835: Head2: Special Cases or Exceptions	66
66239: Head3: Product Component Special Cases	66
18126: Head3: Shared Component Special Cases	66
74193: ChapTitle: Upgrading System Components	69
89815: Procedure: % Applying Patches	70

79265: Head2: General Considerations	70
65274: Head2: Synchronizing Shared Components	70
94148: Head2: Synchronizing All Shared Components	72
40353: Head2: Solaris 10 Zone Considerations	72
22759: Head1: Shared Component Upgrade Procedure	75
24723: Head1: Special Upgrade Procedures	75
81664: Head2: Upgrading J2SE Packages	76
29469: TableCaption: Table 6-3 Application Server version verification outputs	77
38561: Head3: Common Agent Container (CACAO)	78
68144: Step1: 1. If the current installation uses custom configuration settings (for example,	78
62821: Step1+: 5. Apply any custom configuration settings previously captured in Step 1 on	79
70527: Step1+: 8. FOOIf you upgraded J2SE to J2SE Version 5, run the rebuild-dependencies	79
47678: Head1: Manual Upgrade Procedures	80
74193: ChapTitle: Upgrading System Components	81
17885: Head1: Preparing for Upgrades	82
41290: Head1: Upgrading Shared Components	82
34673: Procedure: % Patch Contents	82
73321: Head1: Message Queue Upgrade Information	82
23459: Head1: Upgrading to Administration Server 5.2	82
15541: Head2: About Java ES Release 4 Access Manager	82
46544: Head2: Access Manager Upgrade Roadmap	83
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	83
26267: Head2: Access Manager Data	84
18668: Head2: Sun Cluster Upgrade Strategy	85
26959: Head2: Compatibility Issues	85
43330: Head2: Access Manager Dependencies	85
18756: Head1: Upgrading Access Manager from Java ES Release 3	86
46384: Head2: Introduction	86

93913: Head2: Full Access Manager Upgrade	87
90948: Head2: Before You Upgrade	87
35243: Head4: Verify Current Version Information	89
29469: TableCaption: Table 6-3 Application Server version verification outputs	89
57504: Head4: Prepare the Cluster Node for Upgrade	89
49065: Head4: Upgrade the Operating System	90
44778: Head3: Upgrading Access Manager Dependencies	90
39931: Head3: Obtain the Required Information	90
49530: Head2: Access Manager Upgrade Procedures	91
34640: Head4: Upgrade Considerations	91
19412: Head4: Upgrade Procedure	91
79521: Head2: Verifying the Upgrade	92
95616: Head2: Post-Upgrade Tasks	92
71706: Head2: Upgrade Rollback	93
44595: ChapTitle: Directory Proxy Server	95
69359: Note: Note	95
17885: Head1: Preparing for Upgrades	96
41290: Head1: Upgrading Shared Components	96
34673: Procedure: % Patch Contents	96
73321: Head1: Message Queue Upgrade Information	96
23459: Head1: Upgrading to Administration Server 5.2	96
15541: Head2: About Java ES Release 4 Access Manager	96
46544: Head2: Access Manager Upgrade Roadmap	96
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	96
26267: Head2: Access Manager Data	97
23608: Head2: Portal Server Upgrade Strategy	97
26959: Head2: Compatibility Issues	97
43330: Head2: Access Manager Dependencies	98

18756: Head1: Upgrading Access Manager from Java ES Release 3	98
46384: Head2: Introduction	98
87678: Head2: Versions 3.1 Sun Cluster Geo Upgrade	99
90948: Head2: Before You Upgrade	99
30517: Head4: Verify Current Version Information	100
29469: TableCaption: Table 6-3 Application Server version verification outputs	100
94955: Head4: Prepare a Cluster for an Upgrade	100
86699: Step1: 1. Ensure that eh cluster is functioning properly.	100
74111: Step1+: 3. Remove all application resource groups from protection groups.	101
44778: Head3: Upgrading Access Manager Dependencies	101
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	101
19147: Head3: Back Up Directory Server	102
39931: Head3: Obtain the Required Information	102
49530: Head2: Access Manager Upgrade Procedures	102
34640: Head4: Upgrade Considerations	102
19412: Head4: Upgrade Procedure	102
34896: Step1: 1. Log in as root or become superuser.	103
90067: Step1+: 2. Shut down Sun Cluster Geo 3.1.	103
74138: Step1+: 6. Install all the required Sun Cluster Geo patches.	104
61615: Step1+: 6. Re-start Release 5 Sun Cluster Geo.	104
79521: Head2: Verifying the Upgrade	105
95616: Head2: Post-Upgrade Tasks	105
71706: Head2: Upgrade Rollback	105
74193: ChapTitle: Upgrading System Components	107
17885: Head1: Preparing for Upgrades	109
41290: Head1: Upgrading Shared Components	109
34673: Procedure: % Patch Contents	109
73321: Head1: Message Queue Upgrade Information	109
23459: Head1: Upgrading to Administration Server 5.2	109

15541: Head2: About Java ES Release 4 Access Manager	109
46544: Head2: Access Manager Upgrade Roadmap	109
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	109
26267: Head2: Access Manager Data	111
23608: Head2: Portal Server Upgrade Strategy	112
26959: Head2: Compatibility Issues	112
43330: Head2: Access Manager Dependencies	112
18756: Head1: Upgrading Access Manager from Java ES Release 3	114
46384: Head2: Introduction	114
93913: Head2: Full Access Manager Upgrade	115
90948: Head2: Before You Upgrade	115
34684: Head4: Verify Current Version Information	115
29469: TableCaption: Table 6-3 Application Server version verification outputs	115
44778: Head3: Upgrading Access Manager Dependencies	116
39931: Head3: Obtain the Required Information	116
56542: Head4: Create DS Image (Optional)	116
49530: Head2: Access Manager Upgrade Procedures	116
34640: Head4: Upgrade Considerations	117
19412: Head4: Upgrade Procedure	117
79283: Step1+: 7. Create a Directory Server instance.	120
28818: Step1+: 8. Migrate Release 4 data to the Release 5 Directory Server instance.	120
69359: Note: Note	121
79521: Head2: Verifying the Upgrade	121
95616: Head2: Post-Upgrade Tasks	122
71706: Head2: Upgrade Rollback	122
12921: Head1: Multiple Instance Upgrades	122
41813: Head2: Upgrading Directory Server as a Data Service in a Cluster	123
70823: Head1: Upgrading Directory Server from Java ES Release 3	123

19472: Head1: Upgrading Access Manager from Java ES Release 2	123
44595: ChapTitle: Directory Proxy Server	125
17885: Head1: Preparing for Upgrades	127
41290: Head1: Upgrading Shared Components	127
34673: Procedure: % Patch Contents	127
73321: Head1: Message Queue Upgrade Information	127
23459: Head1: Upgrading to Administration Server 5.2	127
15541: Head2: About Java ES Release 4 Access Manager	127
46544: Head2: Access Manager Upgrade Roadmap	127
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	128
26267: Head2: Access Manager Data	129
23608: Head2: Portal Server Upgrade Strategy	129
26959: Head2: Compatibility Issues	130
43330: Head2: Access Manager Dependencies	131
18756: Head1: Upgrading Access Manager from Java ES Release 3	132
46384: Head2: Introduction	132
93913: Head2: Full Access Manager Upgrade	133
90948: Head2: Before You Upgrade	133
10228: Head4: Verify Current Version Information	133
29469: TableCaption: Table 6-3 Application Server version verification outputs	133
44778: Head3: Upgrading Access Manager Dependencies	134
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	134
39931: Head3: Obtain the Required Information	134
49530: Head2: Access Manager Upgrade Procedures	134
34640: Head4: Upgrade Considerations	135
19412: Head4: Upgrade Procedure	135
86649: Step1+: 3. Shut down all Java ES components dependent on the Directory Server,	135
24850: Step1+: 4. Create a Directory Proxy Server instance.	137

26229: Step1+: 5. If desired, map Release 4 configuration attributes to the Release 5 Directory	137
79521: Head2: Verifying the Upgrade	137
95616: Head2: Post-Upgrade Tasks	137
71706: Head2: Upgrade Rollback	138
12921: Head1: Multiple Instance Upgrades	138
21426: Head1: Upgrading Directory Proxy Server from Java ES Release 3	139
19472: Head1: Upgrading Access Manager from Java ES Release 2	140
74193: ChapTitle: Upgrading System Components	141
17885: Head1: Preparing for Upgrades	142
41290: Head1: Upgrading Shared Components	142
34673: Procedure: % Patch Contents	142
73321: Head1: Message Queue Upgrade Information	142
23459: Head1: Upgrading to Administration Server 5.2	142
15541: Head2: About Java ES Release 4 Access Manager	142
46544: Head2: Access Manager Upgrade Roadmap	143
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	143
26267: Head2: Access Manager Data	143
23608: Head2: Portal Server Upgrade Strategy	144
26959: Head2: Compatibility Issues	144
63673: TableCaption: Table 7-3 Web Server Default Names	145
43330: Head2: Access Manager Dependencies	145
18756: Head1: Upgrading Access Manager from Java ES Release 3	146
46384: Head2: Introduction	146
93913: Head2: Full Access Manager Upgrade	147
90948: Head2: Before You Upgrade	147
23715: Head4: Verify Current Version Information	147
29469: TableCaption: Table 6-3 Application Server version verification outputs	147
44778: Head3: Upgrading Access Manager Dependencies	148

19147: Head3: Back Up Directory Server	148
39931: Head3: Obtain the Required Information	148
49530: Head2: Access Manager Upgrade Procedures	148
34640: Head4: Upgrade Considerations	148
19412: Head4: Upgrade Procedure	151
91177: Step1+: 3. Stop all running instances of Web Server and the Administration Server.	151
89234: Step2+: e. If you choose configure now	152
37914: Step2+: f. If you choose configure later:	153
54074: Step3+: II. Run the configureServer script.	155
91653: Step1+: 4. Start the Web Server Administration Server service.	155
34612: Step1+: 5. Migrate Release 4 Web Server instances to Release 5 configurations.	155
17030: TableCaptionIndent: Table 6-4 wadm migrate-server Command Options and Arguments	156
59476: TableCaptionIndent: Table 6-5 wadm migrate-server Command Options	158
92706: Step2+: c. If the target instance already exists as the default instance, then you can	161
93575: TableCaptionIndent: Table 6-7 wadm deploy-cofig Command Options and Operands	161
71778: Step1+: 7. Start each Release 5 instance.	162
79521: Head2: Verifying the Upgrade	162
95616: Head2: Post-Upgrade Tasks	163
62873: Head4: Migrating Web Server 6.1 docroot content	163
71158: Head4: Migrating webdav collection information	164
10590: Head4: Migrating Log files	164
85187: Head4: Migrating 3rd party NSAPI plug-ins	164
39918: Head4: Changing the search collection document root	165
70227: Head4: Customizing command-line scripts	166
71706: Head2: Upgrade Rollback	166
19472: Head1: Upgrading Access Manager from Java ES Release 2	168
24060: Head1: Upgrading Web Server from Java ES Release 2	169
44595: ChapTitle: Directory Proxy Server	171

69359: Note: Note	171
17885: Head1: Preparing for Upgrades	172
41290: Head1: Upgrading Shared Components	172
34673: Procedure: % Patch Contents	172
73321: Head1: Message Queue Upgrade Information	172
23459: Head1: Upgrading to Administration Server 5.2	172
15541: Head2: About Java ES Release 4 Access Manager	172
46544: Head2: Access Manager Upgrade Roadmap	172
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	172
26267: Head2: Access Manager Data	173
23608: Head2: Portal Server Upgrade Strategy	173
26959: Head2: Compatibility Issues	173
43330: Head2: Access Manager Dependencies	173
18756: Head1: Upgrading Access Manager from Java ES Release 3	174
46384: Head2: Introduction	174
93913: Head2: Full Access Manager Upgrade	174
90948: Head2: Before You Upgrade	175
77155: Head4: Verify Current Version Information	175
29469: TableCaption: Table 6-3 Application Server version verification outputs	175
44778: Head3: Upgrading Access Manager Dependencies	175
19147: Head3: Back Up Directory Server	176
39931: Head3: Obtain the Required Information	176
49530: Head2: Access Manager Upgrade Procedures	176
19412: Head4: Upgrade Procedure	176
79521: Head2: Verifying the Upgrade	177
95616: Head2: Post-Upgrade Tasks	178
71706: Head2: Upgrade Rollback	178
12921: Head1: Multiple Instance Upgrades	178

74193: ChapTitle: Upgrading System Components	179
17885: Head1: Preparing for Upgrades	181
41290: Head1: Upgrading Shared Components	181
34673: Procedure: % Patch Contents	181
73321: Head1: Message Queue Upgrade Information	181
23459: Head1: Upgrading to Administration Server 5.2	181
15541: Head2: About Java ES Release 4 Access Manager	181
36281: Head2: HADB Upgrade Roadmap	181
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	181
29711: Head2: HADB Data	182
23608: Head2: Portal Server Upgrade Strategy	182
26959: Head2: Compatibility Issues	182
18756: Head1: Upgrading Access Manager from Java ES Release 3	184
46384: Head2: Introduction	184
93913: Head2: Full Access Manager Upgrade	185
90948: Head2: Before You Upgrade	185
43372: Head4: Verify Current Version Information	185
29469: TableCaption: Table 6-3 Application Server version verification outputs	185
44778: Head3: Upgrading Access Manager Dependencies	186
19147: Head3: Back Up Directory Server	186
39931: Head3: Obtain the Required Information	186
49530: Head2: Access Manager Upgrade Procedures	186
34640: Head4: Upgrade Considerations	186
32630: TableCaption: Table 2-2 Package Versions for Upgrading Shared Components on Solaris Platforms	187
79521: Head2: Verifying the Upgrade	189
95616: Head2: Post-Upgrade Tasks	190
71706: Head2: Upgrade Rollback	191
88733: Head1: Upgrading HADB from Java ES Release 3	192

74193: ChapTitle: Upgrading System Components	193
17885: Head1: Preparing for Upgrades	194
41290: Head1: Upgrading Shared Components	194
34673: Procedure: % Patch Contents	194
73321: Head1: Message Queue Upgrade Information	194
23459: Head1: Upgrading to Administration Server 5.2	194
15541: Head2: About Java ES Release 4 Access Manager	194
46544: Head2: Access Manager Upgrade Roadmap	195
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	195
26267: Head2: Access Manager Data	196
20617: TableCaptionWide: Table 8-2 Message Queue Data Usage (Solaris OS)	196
23608: Head2: Portal Server Upgrade Strategy	197
26959: Head2: Compatibility Issues	197
43330: Head2: Access Manager Dependencies	197
18756: Head1: Upgrading Access Manager from Java ES Release 3	199
46384: Head2: Introduction	199
93913: Head2: Full Access Manager Upgrade	200
90948: Head2: Before You Upgrade	200
67437: Head4: Verify Current Version Information	200
29469: TableCaption: Table 6-3 Application Server version verification outputs	201
44778: Head3: Upgrading Access Manager Dependencies	201
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	201
49130: Head4: Back Up Message Queue	202
49530: Head2: Access Manager Upgrade Procedures	202
79521: Head2: Verifying the Upgrade	203
95616: Head2: Post-Upgrade Tasks	203
71706: Head2: Upgrade Rollback	204
12921: Head1: Multiple Instance Upgrades	205

62991: Head1: Upgrading Message Queue from Java ES Release 3	206
19472: Head1: Upgrading Access Manager from Java ES Release 2	207
57508: Head2: Compatibility Issues	208
12331: Head3: Protocol Compatibility	208
28321: Head3: Broker Compatibility	208
16480: Head3: Administered Objects	209
95774: Head3: Administration Tool Compatibility	210
76701: Head3: Client Compatibility	210
36929: Head2: Release 2 Message Queue Upgrade	210
86655: Head4: Verify Current Version Information (Solaris Systems)	211
38575: Head4: Upgrade Message Queue Dependencies	211
90377: Head4: Back Up Message Queue	212
60583: Head3: Upgrading Release 2 Message Queue (Solaris)	212
59119: Head3: Upgrading Release 2 Message Queue (Linux)	214
95739: Step1+: 6. Migrate broker instance data using the following command:	215
45153: Step1+: 7. Run the mqupgrade script.	215
79935: Head3: Installing the sun-mq-compat Package	216
61002: Head3: Verifying the Message Queue Upgrade	216
54290: Head3: Post-Upgrade Tasks	216
76601: Head3: Rolling Back the Upgrade	217
74193: ChapTitle: Upgrading System Components	219
34104: Head1: Overview of Application Server Upgrades	221
15541: Head2: About Java ES Release 4 Access Manager	221
46544: Head2: Access Manager Upgrade Roadmap	221
33786: TableCaptionWide: Table 11-2 Upgrade Paths to Java ES 5 (Release 5): Application Server Enterprise Edition 8.2	222
30603: TableCaptionWide: Table 11-3 Upgrade Paths for Application Server Versions Bundled with Solaris Operating System	223
26267: Head2: Access Manager Data	224
80642: TableCaptionWide: Table 10-3 Application Server Data Usage	224

23608: Head2: Portal Server Upgrade Strategy	225
26959: Head2: Compatibility Issues	225
43330: Head2: Access Manager Dependencies	225
16247: Note: Note	226
18756: Head1: Upgrading Access Manager from Java ES Release 3	227
46384: Head2: Introduction	227
93913: Head2: Full Access Manager Upgrade	228
90948: Head2: Before You Upgrade	228
88295: Head4: Verify Current Version Information	228
29469: TableCaption: Table 6-3 Application Server version verification outputs	229
44778: Head3: Upgrading Access Manager Dependencies	229
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	229
19147: Head3: Back Up Directory Server	230
39931: Head3: Obtain the Required Information	230
49530: Head2: Access Manager Upgrade Procedures	230
34640: Head4: Upgrade Considerations	230
19412: Head4: Upgrade Procedure	230
86649: Step1+: 3. Shut down all Java ES components dependent on the Directory Server,	231
79521: Head2: Verifying the Upgrade	232
95616: Head2: Post-Upgrade Tasks	232
71706: Head2: Upgrade Rollback	233
84321: Head1: Upgrading Application Server from Java ES Release 3	234
19472: Head1: Upgrading Access Manager from Java ES Release 2	235
20329: Head2: Introduction	235
69047: Head2: Release 2 Application Server Upgrade	236
13674: Head4: Solaris Only: Manually Remove the Application Server Packages Bundled	237
26914: Head4: Verify Current Version Information	237
47180: Head4: Upgrade Application Server Dependencies	237
58344: Head4: Back Up Application Server Data	239

98757: Head4: Obtain Required Configuration Information and Passwords	239
81692: Head3: Upgrading Release 2 Application Server	239
16801: Head4: Upgrade Procedure	239
96166: Step1+: 2. If Java ES shared components have been upgraded to Release 5 (in particular	240
41022: Step1+: 3. Stop all Application Server and related processes.	240
51295: Step1+: 3. Install Release 4 Application Server using the Java ES installer, choosing the	240
25486: Step2+: c. Select Application Server from the component selection panel.	240
23402: Step2+: d. Specify an installation directory different from that in which Release 2 was	241
40237: Step1+: 5. Perform the following post-install procedure:	241
53630: Step1+: 5. Run the asupgrade utility.	242
86242: Step1+: 4. Identify both target and source installation directories, for example:	242
36701: Step1+: 9. Start the Domain Administration Server (DAS).	243
49085: Step1+: 10. Restart upgraded Application Server instances.	243
23993: Head3: Upgrading Release 2 Application Server (Linux)	244
47178: Head3: Post-Upgrade Tasks	244
24193: Head4: Correct the Reference to JSS	244
35947: Head4: Migration of Release 2 J2EE Components	245
95586: Head3: Rolling Back the Upgrade	245
14447: Head2: 7. An Illustrative Example: Install Application Server in a Sparse Root Zone	246
44595: ChapTitle: Directory Proxy Server	249
69359: Note: Note	249
17885: Head1: Preparing for Upgrades	251
41290: Head1: Upgrading Shared Components	251
34673: Procedure: % Patch Contents	251
73321: Head1: Message Queue Upgrade Information	251
23459: Head1: Upgrading to Administration Server 5.2	251
15541: Head2: About Java ES Release 4 Access Manager	251
46544: Head2: Access Manager Upgrade Roadmap	251

57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	251
26267: Head2: Access Manager Data	252
23608: Head2: Portal Server Upgrade Strategy	252
26959: Head2: Compatibility Issues	252
43330: Head2: Access Manager Dependencies	253
18756: Head1: Upgrading Access Manager from Java ES Release 3	254
46384: Head2: Introduction	254
93913: Head2: Full Access Manager Upgrade	255
90948: Head2: Before You Upgrade	255
24956: Head4: Verify Current Version Information	255
29469: TableCaption: Table 6-3 Application Server version verification outputs	256
44778: Head3: Upgrading Access Manager Dependencies	256
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	256
19147: Head3: Back Up Directory Server	257
39931: Head3: Obtain the Required Information	257
49530: Head2: Access Manager Upgrade Procedures	257
19412: Head4: Upgrade Procedure	257
61791: Step1+: 6. Upgrade and configure the Release 5 Service Registry.	258
79521: Head2: Verifying the Upgrade	260
95616: Head2: Post-Upgrade Tasks	261
71706: Head2: Upgrade Rollback	261
12921: Head1: Multiple Instance Upgrades	262
74193: ChapTitle: Upgrading System Components	263
17885: Head1: Preparing for Upgrades	264
41290: Head1: Upgrading Shared Components	264
34673: Procedure: % Patch Contents	264
73321: Head1: Message Queue Upgrade Information	264
23459: Head1: Upgrading to Administration Server 5.2	264

15541: Head2: About Java ES Release 4 Access Manager	264
46544: Head2: Access Manager Upgrade Roadmap	264
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	264
26267: Head2: Access Manager Data	265
23608: Head2: Portal Server Upgrade Strategy	265
26959: Head2: Compatibility Issues	266
43330: Head2: Access Manager Dependencies	266
18756: Head1: Upgrading Access Manager from Java ES Release 3	267
78545: Head2: Release 4 Web Proxy Server Upgrade	268
88643: Head4: Verify Current Version Information	268
93575: TableCaption: Table 11-3 Web Proxy Server Version Verification Outputs	268
95242: Head4: Upgrade Web Proxy Server Dependencies	269
49984: Head4: Back Up Web Proxy Server Data	269
57637: Head4: Obtain Required Configuration Information and Passwords	269
93656: Head3: Upgrading Release 4 Web Proxy Server (Solaris)	269
16936: TableCaptionIndent: Table 4-3 Patches to Upgrade Administration Server, Directory Server, and	269
93280: Head4: Upgrade Procedure (Solaris)	270
91177: Step1+: 3. Stop all running instances of Web Server and the Administration Server.	270
69482: Step2: a. Apply the Administration Server patches.	270
69739: Head3: Upgrading Web Server (Linux)	271
14399: Head4: Upgrade Considerations (Linux)	271
54062: TableCaptionIndent: Table 4-4 Patches to Upgrade Administration Server Directory Server, and	271
97364: Head4: Upgrade Procedure (Linux)	271
84274: Head3: Rolling Back the Upgrade (Solaris)	273
64922: Step1+: 2. Stop all running instances of Web Proxy Server and the Administration Server.	273
29419: Head1: Upgrading Web Proxy Server from Version 3.6	274

46384: Head2: Introduction	274
55960: Head2: Version 3.6 Web Proxy Server Upgrade	275
90948: Head2: Before You Upgrade	275
39518: Head4: Verify Current Version Information	275
29676: TableCaption: Table 11-6 Web Proxy Server Version Verification Outputs	275
44778: Head3: Upgrading Access Manager Dependencies	276
19147: Head3: Back Up Directory Server	276
39931: Head3: Obtain the Required Information	276
49530: Head2: Access Manager Upgrade Procedures	276
34640: Head4: Upgrade Considerations	276
19412: Head4: Upgrade Procedure	276
97789: Step2+: d. Click the Migrate button.	278
79521: Head2: Verifying the Upgrade	278
95616: Head2: Post-Upgrade Tasks	278
71706: Head2: Upgrade Rollback	279
74193: ChapTitle: Upgrading System Components	281
17885: Head1: Preparing for Upgrades	282
41290: Head1: Upgrading Shared Components	282
34673: Procedure: % Patch Contents	282
73321: Head1: Message Queue Upgrade Information	282
23459: Head1: Upgrading to Administration Server 5.2	282
15541: Head2: About Java ES Release 4 Access Manager	282
46544: Head2: Access Manager Upgrade Roadmap	283
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	283
26267: Head2: Access Manager Data	285
22953: TableCaptionWide: Table 11-2 Access Manager Data Usage	285
23608: Head2: Portal Server Upgrade Strategy	286
26959: Head2: Compatibility Issues	286

43330: Head2: Access Manager Dependencies	287
23141: TableCaption: Table 11-3 Web Container Upgrade Scenarios for Access Manager Upgrade	288
18756: Head1: Upgrading Access Manager from Java ES Release 3	290
46384: Head2: Introduction	290
93913: Head2: Full Access Manager Upgrade	291
90948: Head2: Before You Upgrade	291
23760: Head4: Verify Current Version Information	292
29469: TableCaption: Table 6-3 Application Server version verification outputs	292
44778: Head3: Upgrading Access Manager Dependencies	292
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	292
19147: Head3: Back Up Directory Server	293
27083: Head4: Back Up Release 4 Access Manager Configuration Information	293
61806: Head2: Backing up Web Container Files	294
53828: Head3: Backing Up Access Manager Release 3	294
81910: Head4: Back Up Custom Localization Files	295
39931: Head3: Obtain the Required Information	295
49530: Head2: Access Manager Upgrade Procedures	295
16910: Step1+: 2. Remove the Java ES Release 4 Version of Access Manager. Use the	295
31541: Step1+: 7. Update the directory structure and schema. Use the amupgrade script.	296
30579: Step1+: 3. Upgrade mobile access software.	296
13934: TableCaptionIndent: Table 6-3 Patches to Upgrade Messaging Server on Solaris	296
93040: Head3: Remove the Java ES Release 3 Version of Access Manager	297
35655: Step1+: 2. If the upgrade to Release 5 needs to be localized, remove Release 4 localization	298
24529: Step2: a. Check for localization packages.	298
78467: Head3: Install Java ES Release 4 Version of Access Manager	299
91206: Head3: Re-apply Customized JSPs for Access Manager	300
49148: Head3: Re-deploy Access Manager Web Applications	300
62405: Step2+: d. If Access Manager is deployed in Release 5 Web Server, disable all Java ES	301

15015: Head3: Upgrade the Directory Schema	305
93497: Step1+: 2. Run the amupgrade script.	306
79521: Head2: Verifying the Upgrade	306
95616: Head2: Post-Upgrade Tasks	307
78316: Head4: Migrating to Realm Mode	308
55903: Head4: Security Assertion Markup Language	308
97810: Head4: Update Patches	308
71706: Head2: Upgrade Rollback	308
12921: Head1: Multiple Instance Upgrades	309
31938: FigureCaption: Figure 14-1 Typical Deployment Architecture for Multiple Access Manager Instances	309
66117: Head2: Access Manager SDK-only Upgrades	311
94723: Head2: Access Manager SDK Upgrade Procedures	312
62989: Head2: Verifying the Access Manager SDK Upgrade	313
56774: Head1: Upgrading Access Manager from Java ES Release 3	315
23590: Head2: Release 3 Access Manager Upgrade	315
59477: Head2: Multiple Instance Release 3 Access Manager Upgrade	315
16251: FigureCaption: Figure 14-2 Example Deployment Architecture for Multiple Access Manager Instances	316
19472: Head1: Upgrading Access Manager from Java ES Release 2	320
19884: Head2: Pre-Upgrade Tasks	320
24162: Head3: Upgrade Access Manager Dependencies	321
95303: Head3: Upgrade Directory Schema	321
21940: Head3: Re-index the Directory	321
35795: Head2: Release 2 Access Manager Upgrade	323
24401: Head3: Upgrading Messaging Server (Solaris)	323
60105: Head3: Upgrading Access Manager: Application Server Web Container	323
77541: Step1: 1. Upgrade Access Manager mobile access software.	325
83145: Step1+: 2. Remove the Java ES Release 2 Version of Access Manager.	326
18497: Step1+: 3. If the upgrade to Release 5 needs to be localized, remove the Release 2	327

63603: Step1+: 4. Install the Java ES Release 5 Version of Access Manager.	327
12988: Step1+: 6. Check that Directory Server is running.	329
49202: Step1+: 7. Start the following Application Server instances:	329
78174: Step1+: 8. Undeploy Access Manager, reconfigure, and re-deploy into the Application	329
13868: Step1+: 9. Verify that Access Manager classpath-suffix and server-classpath	332
72142: Step1+: 12. Update the directory structure and schema.	332
32139: Step1+: 10. Stop the Domain Administration Server (DAS) and node agent that were	334
61227: Step1+: 11. Restart the the Domain Administration Server (DAS), node agent, and server	334
86085: Head2: Multiple Instance Upgrade	335
74193: ChapTitle: Upgrading System Components	337
17885: Head1: Preparing for Upgrades	339
41290: Head1: Upgrading Shared Components	339
34673: Procedure: % Patch Contents	339
73321: Head1: Message Queue Upgrade Information	339
23459: Head1: Upgrading to Administration Server 5.2	339
15541: Head2: About Java ES Release 4 Access Manager	339
46544: Head2: Access Manager Upgrade Roadmap	339
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	340
26267: Head2: Access Manager Data	340
23608: Head2: Portal Server Upgrade Strategy	341
26959: Head2: Compatibility Issues	342
43330: Head2: Access Manager Dependencies	342
49667: Head3: Selective Upgrade Issues	343
77725: TableCaptionIndent: Table 17-5 Portal Server Upgrade Scenarios for Different Web Containers	344
18756: Head1: Upgrading Access Manager from Java ES Release 3	346
46384: Head2: Introduction	346
93913: Head2: Full Access Manager Upgrade	348

90948: Head2: Before You Upgrade	349
86427: Head4: Verify Current Version Information	349
29469: TableCaption: Table 6-3 Application Server version verification outputs	349
44778: Head3: Upgrading Access Manager Dependencies	349
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	350
39931: Head3: Obtain the Required Information	351
67657: TableCaptionIndent: Table 17-5 Information Requested by psupgrade Script for Various Upgrade	351
16146: Head4: Back Up Release 4 Portal Server Configuration Information	353
60248: Head4: Note Java Virtual Machine (JVM) Settings	353
24690: Head4: Remove Configuration for Load Balancer	354
57135: Head4: Remove Configuration for Directory Proxy Server	355
49530: Head2: Access Manager Upgrade Procedures	355
34640: Head4: Upgrade Considerations	355
19412: Head4: Upgrade Procedure	356
56828: Step1+: 3. If not already running, start Portal Server by starting the web container to	356
41845: Step1+: 4. Set two environment variables needed by the psupgrade script:	357
89837: Step1+: 4. Run the psupgrade script.	357
69739: Head3: Upgrading Web Server (Linux)	359
14399: Head4: Upgrade Considerations (Linux)	359
97364: Head4: Upgrade Procedure (Linux)	359
94383: Step1+: 5. If not already running, start Portal Server by starting the web container to	360
14016: Step1+: 8. Run the psupgrade script from the Java ES Release 5 distribution.	361
79521: Head2: Verifying the Upgrade	362
95616: Head2: Post-Upgrade Tasks	363
95668: Head4: Migrate Custom web-src Data	363
27601: Head4: Redeploy Custom Portlet Applications	364
63225: Head4: Migrate Customized Portlet Applications	364
13908: Step1+: 2. Locate the filesharing portlet application.	365

69773: Step1+: 5. Redeploy the filesharing portlet application.	365
59153: Step2+: c. Go to the following directory (depending on web container):	365
98193: Step2+: d. Open the sun-web.xml file and add the following line just before the last	366
80829: Head4: Correct Access to Search Server	366
46403: Head4: Restore Configuration for Directory Proxy Server	366
75598: Head3: Manually Register Portal Server Secure Remote Access	367
13217: Head3: Enabling URLScrapper Channel	367
78603: Step1+: 4. Locate the entire XML portion starting from:	367
66019: Head4: Logout Page	370
71706: Head2: Upgrade Rollback	370
79353: Head3: Rolling Back the Upgrade (Linux)	372
12921: Head1: Multiple Instance Upgrades	372
31938: FigureCaption: Figure 14-1 Typical Deployment Architecture for Multiple Access Manager Instances	374
72247: Step1: 1. If you are upgrading Release 4 Access Manager to Release 5, perform a rolling	374
16198: Step2+: c. Upgrade Access Manager SDK 1B to Release 5.	375
45043: Step2+: d. Upgrade Portal Server 1 to Release 5.	375
32637: Head1: Upgrading Portal Server from Java ES Release 3	377
24651: Head2: Release 3 Pre-Upgrade Task: Upgrading Portal Server Dependencies	377
36852: Head2: Release 3 Portal Server Upgrade	378
19573: Head2: Release 3 Post-Upgrade Tasks	378
76092: Head3: Subscribing a Discussion	378
88282: Head2: Multiple Instance Upgrades	379
73569: Head1: Upgrading Portal Server from Java ES Release 2	380
33156: Head2: Pre-Upgrade Tasks	380
79129: Head2: Upgrading Release 2 Portal Server	381
24401: Head3: Upgrading Messaging Server (Solaris)	381
60105: Head3: Upgrading Access Manager: Application Server Web Container	382
47403: Step1+: 4. If not already running, start Portal Server by starting the web container to	382

30452: Step1+: 9. Run the psupgrade script from the Java ES Release 5 distribution.	384
32139: Step1+: 10. Stop the Domain Administration Server (DAS) and node agent that were	385
64787: Head2: Release 2 Post-Upgrade Tasks	386
78956: Head3: Single Sign-on Configuration	386
26757: Head3: Enabling the URLScrapper Channel	390
65685: Head3: Delete Gateway Service Entry	390
99094: Head2: Multiple Instance Upgrades	390
18474: Head1: Upgrading Portal Server from the Interim Feature	391
20105: Head2: Introduction	391
71392: TableCaptionIndent: Table 17-6 Patches to Upgrade Portal Server IFR to Release 5 on Solaris	391
66302: Head2: Portal Server IFR 7.0 Upgrade	392
20319: Head3: Pre-Upgrade Tasks	393
86903: Head3: Upgrading Portal Server IFR 7.0 (Solaris)	393
93710: Head4: Upgrade Considerations (Solaris)	393
15809: Head4: IFR 7 Upgrade Procedure (Solaris)	393
56479: Step1+: 4. If not already running, start Portal Server by starting the web container to	394
21387: Step1+: 4. Obtain the required patch, based on Table 17-6.	394
69482: Step2: a. Apply the Administration Server patches.	394
10785: Step1+: 6. Confirm that the patch upgrade was successful:	395
12340: Step1+: 11. Run the psupgrade script.	395
42263: Head3: Upgrading IFR 7 Portal Server (Linux)	396
59024: Head3: Upgrading Portal Server IFR 7.0 (Linux)	396
77944: Step1+: 4. If not already running, start Portal Server by starting the web container to	397
30186: Step1+: 11. Run the psupgrade script.	398
25105: Head3: Verifying the Upgrade	399
22792: Head3: Post-Upgrade Tasks	400
96066: Head4: Configuration of Common Agent Container Shared Component	400
48904: Head4: Enabling the Java ES Monitoring Framework	401

84419: Head4: Upgrade in Application Server Web Container	402
19754: Head4: Upgrade in Web Server Web Container	403
82941: Step1+: 4. Delete the Portal Server IFR instance.	404
82315: Head4: Redeploy Custom Portlet Applications	404
41727: Head4: Migrate Customized Portlet Applications	404
72947: Head4: Manual Migration of Struts-based Portlets	406
78568: Head3: Rolling Back the Upgrade (Solaris)	407
91734: Head3: Rolling Back the Upgrade (Linux)	409
94840: Head2: Multiple Instance Upgrades	409
74193: ChapTitle: Upgrading System Components	411
17885: Head1: Preparing for Upgrades	413
41290: Head1: Upgrading Shared Components	413
34673: Procedure: % Patch Contents	413
73321: Head1: Message Queue Upgrade Information	413
23459: Head1: Upgrading to Administration Server 5.2	413
15541: Head2: About Java ES Release 4 Access Manager	413
46544: Head2: Access Manager Upgrade Roadmap	413
57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1	414
26267: Head2: Access Manager Data	414
23608: Head2: Portal Server Upgrade Strategy	415
26959: Head2: Compatibility Issues	415
43330: Head2: Access Manager Dependencies	416
23142: Head3: Selective Upgrade Issues	417
18756: Head1: Upgrading Access Manager from Java ES Release 3	418
46384: Head2: Introduction	418
21678: Bullet1: • Upgrade Dependencies. While Portal Server has dependencies on a number	419
93913: Head2: Full Access Manager Upgrade	420
90948: Head2: Before You Upgrade	420

47076: Head4: Verify Current Version Information	420
29469: TableCaption: Table 6-3 Application Server version verification outputs	421
44778: Head3: Upgrading Access Manager Dependencies	421
32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared	422
43322: Head4: Back Up Release 4 Portal Server Secure Remote Access Configuration	422
24690: Head4: Remove Configuration for Load Balancer	422
57135: Head4: Remove Configuration for Directory Proxy Server	423
39931: Head3: Obtain the Required Information	423
49530: Head2: Access Manager Upgrade Procedures	424
34640: Head4: Upgrade Considerations	424
19412: Head4: Upgrade Procedure	425
92871: Step1+: 3. Stop any instances of the Gateway, Rewriter Proxy, or Netlet Proxy that are	425
41845: Step1+: 4. Set two environment variables needed by the psupgrade script:	425
35135: Step1+: 8. Run the psupgrade script from the Java ES Release 5 distribution.	426
69739: Head3: Upgrading Web Server (Linux)	427
14399: Head4: Upgrade Considerations (Linux)	427
97364: Head4: Upgrade Procedure (Linux)	427
17364: Step1+: 8. Run the psupgrade script from the Java ES Release 5 distribution.	428
79521: Head2: Verifying the Upgrade	429
95616: Head2: Post-Upgrade Tasks	429
92269: Head4: Restore Configuration for Load Balancer	429
44296: Step1+: 2. Set the following parameters in the PortalServer7Config-base/platform.conf.default file:	429
90189: Step1+: 3. Set the following parameter in the PortalServer7Config-base/GWConfig-default.properties file.	430
15493: Head4: Restore Configuration for Directory Proxy Server	430
71826: Head4: Delete Release 4 Localized Providers	430
71706: Head2: Upgrade Rollback	431
79353: Head3: Rolling Back the Upgrade (Linux)	433
12921: Head1: Multiple Instance Upgrades	433

31938: FigureCaption: Figure 14-1 Typical Deployment Architecture for Multiple Access Manager Instances	434
19021: Step1: 1. If you are upgrading Release 4 Access Manager to Release 5, perform a rolling	435
92027: Step1+: 3. Upgrade Portal Server 1.	435
16198: Step2+: c. Upgrade Access Manager SDK 1B to Release 5.	435
45043: Step2+: d. Upgrade Portal Server 1 to Release 5.	435
55497: Step2+: b. Upgrade Access Manager SDK 1A to Release 5.	436
80225: Step2+: c. Upgrade Gateway 1 to Release 5.	436
32637: Head1: Upgrading Portal Server from Java ES Release 3	439
57991: Head2: Upgrading Portal Server Secure Remote Access Dependencies	439
70112: Head2: Upgrading Release 3 Portal Server Secure Remote Access	440
15015: Head2: Multiple Instance Upgrades	440
73569: Head1: Upgrading Portal Server from Java ES Release 2	441
61860: Head2: Release 2 Pre-Upgrade Tasks	441
43743: Head3: Upgrading Portal Server Dependencies.	441
65685: Head3: Delete Gateway Service Entry	442
79129: Head2: Upgrading Release 2 Portal Server	442
76339: Head2: Release 2 Post-Upgrade Tasks	443
64945: Head3: Set PS Domain	443
25975: Head2: Multiple Instance Upgrades	443
18474: Head1: Upgrading Portal Server from the Interim Feature	444
20105: Head2: Introduction	444
33932: TableCaption: Table 16-5 Patches to Upgrade Portal Server Secure Remote Access IFR to Release 5	444
66302: Head2: Portal Server IFR 7.0 Upgrade	445
20319: Head3: Pre-Upgrade Tasks	445
86903: Head3: Upgrading Portal Server IFR 7.0 (Solaris)	445
21387: Step1+: 4. Obtain the required patch, based on Table 17-6.	446
69482: Step2: a. Apply the Administration Server patches.	446
10785: Step1+: 6. Confirm that the patch upgrade was successful:	446

19861: Step1+: 10. Run the psupgrade script.	447
59024: Head3: Upgrading Portal Server IFR 7.0 (Linux)	447
83840: Step1+: 10. Run the psupgrade script.	449
25105: Head3: Verifying the Upgrade	449
22792: Head3: Post-Upgrade Tasks	450
78568: Head3: Rolling Back the Upgrade (Solaris)	450
91734: Head3: Rolling Back the Upgrade (Linux)	450
94840: Head2: Multiple Instance Upgrades	451
30617: ChapNumberA: Appendix B	453
68152: ChapTitleA: Previous Java Enterprise System Releases	453
33080: Head1: Java ES 2003Q4	454
72105: Head3: Sun ONE Administration Server 5.2	454
44958: Head3: Sun ONE Application Server 7, Update 1	454
97608: Head3: Sun ONE Calendar Server 6.0	454
71661: Head3: Sun ONE Directory Server 5.2	454
25410: Head3: Sun ONE Directory Proxy Server 5.2	454
51933: Head3: Sun ONE Identity Server 6.1	454
67613: Head3: Sun ONE Instant Messaging 6.1	454
30041: Head3: Sun ONE Message Queue 3.0.1 Service Pack 2	454
80042: Head3: Sun ONE Messaging Server 6.0	454
92032: Head3: Sun ONE Portal Server 6.2	454
18544: Head3: Sun ONE Portal Server, Secure Remote Access 6.2	454
40736: Head3: Sun ONE Web Server 6.1	454
18017: Head1: Java ES 2004Q2	456
18631: Head1: Java ES 2005Q1	459
98851: Head2: What Are the Component Products?	459
52849: Head2: What Are the Shared Components?	462
46890: Head1: How Do I Get the Java Enterprise System Software?	463
39670: Head1: Java ES 2005Q4 (Release 4)	464

62421: Head2: Release 4 Shared Components	467
81363: Head1: Java ES 2006Q4 (Release 5)	469
80020: Head2: Release 5 Shared Components	472

List of External Cross-References

Dir & Filename	applicationSvr.fm (Head2: Release 2 Application Server Upgrade)	34
Dir & Filename	sharedComps.fm (Head2: Synchronizing All Shared Components)	38
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	51
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	58
Dir & Filename	sunCluster.fm (ChapTitle: Upgrading System Components)	58
Dir & Filename	sunCluster-Geo.fm (ChapTitle: Directory Proxy Server)	58
Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	59
Dir & Filename	directoryProxySvr.fm (ChapTitle: Directory Proxy Server)	59
Dir & Filename	webSvr.fm (ChapTitle: Upgrading System Components)	59
Dir & Filename	javaDB.fm (ChapTitle: Directory Proxy Server)	59
Dir & Filename	highAvailabilityDB.fm (ChapTitle: Upgrading System Components)	59
Dir & Filename	messageQueue.fm (ChapTitle: Upgrading System Components)	59
Dir & Filename	applicationSvr.fm (ChapTitle: Upgrading System Components)	60
Dir & Filename	serviceRegistry.fm (ChapTitle: Directory Proxy Server)	60
Dir & Filename	webProxySvr.fm (ChapTitle: Upgrading System Components)	60
Dir & Filename	accessMgr.fm (ChapTitle: Upgrading System Components).	60
Dir & Filename	portalSvr.fm (ChapTitle: Upgrading System Components)	60
Dir & Filename	portalSvrSRA.fm (ChapTitle: Upgrading System Components).	60
Dir & Filename	portalSvr.fm (Head1: Upgrading Portal Server from the Interim Feature) . .	62

Dir & Filename	sharedComps.fm (Head2: Synchronizing All Shared Components)	64
Dir & Filename	applicationSvr.fm (Head4: Solaris Only: Manually Remove the Application Server Packages Bundled)	66
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	70
Dir & Filename	planning.fm (Head2: Operating System Issues)	70
Dir & Filename	planning.fm (Head1: Preparing for Upgrades)	70
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	85
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	85
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	86
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	90
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	97
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	98
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	99
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	101
Dir & Filename	sunCluster.fm (ChapTitle: Upgrading System Components)	102
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	112
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	112
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	114
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	123
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	123
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	129
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	131
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	132

Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	134
Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	134
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	140
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	140
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	144
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	145
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	146
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	148
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	173
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	173
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	174
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	182
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	197
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	197
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	199
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	201
Dir & Filename	sunCluster.fm (ChapTitle: Upgrading System Components)	201
Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	201
Dir & Filename	WebSvr.fm (ChapTitle: Upgrading System Components)	202
Dir & Filename	ApplicationSvr.fm (ChapTitle: Upgrading System Components)	202
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	212
Dir & Filename	sunCluster.fm (ChapTitle: Upgrading System Components)	212
Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	212
Dir & Filename	WebSvr.fm (ChapTitle: Upgrading System Components)	212

Dir & Filename	ApplicationSvr.fm (ChapTitle: Upgrading System Components).	212
Dir & Filename	planning.fm (Head3: Dual Upgrades: Java ES and Operating System Software) . 214	
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	225
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	225
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	227
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	229
Dir & Filename	messageQueue.fm (ChapTitle: Upgrading System Components).	229
Dir & Filename	highAvailabilityDB.fm (ChapTitle: Upgrading System Components) . . .	229
Dir & Filename	javaDB.fm (ChapTitle: Directory Proxy Server)	229
Dir & Filename	webSvr.fm (ChapTitle: Upgrading System Components)	230
Dir & Filename	planning.fm (Head3: Dual Upgrades: Java ES and Operating System Software) . 236	
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	238
Dir & Filename	messageQueue.fm (Head1: Upgrading Access Manager from Java ES Release 2).	238
Dir & Filename	webSvr.fm (Head1: Upgrading Web Server from Java ES Release 2)	238
Dir & Filename	messageQueue.fm (Head2: Release 2 Message Queue Upgrade)	240
Dir & Filename	planning.fm (Head3: Dual Upgrades: Java ES and Operating System Software) . 244	
Dir & Filename	planning.fm (Head1: Java ES Release 5 and Solaris 10 Zones).	246
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	252
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	253
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	254
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	256
Dir & Filename	javaDB.fm (ChapTitle: Directory Proxy Server)	256
Dir & Filename	ApplicationSvr.fm (ChapTitle: Upgrading System Components).	256
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	265

Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	266
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	267
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	269
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	270
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	276
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	286
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	287
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	290
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	292
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	292
Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	293
Dir & Filename	webSvr.fm (ChapTitle: Upgrading System Components)	293
Dir & Filename	applicationSvr.fm (ChapTitle: Upgrading System Components)	293
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	321
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	321
Dir & Filename	directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) . 321	
Dir & Filename	webSvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) .	321
Dir & Filename	applicationSvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) 321	
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	341
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	342
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	346
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	350

Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	350
Dir & Filename	webSvr.fm (ChapTitle: Upgrading System Components)	350
Dir & Filename	applicationSvr.fm (ChapTitle: Upgrading System Components)	350
Dir & Filename	accessMgr.fm (ChapTitle: Upgrading System Components)	350
Dir & Filename	portalSvrSRA.fm (ChapTitle: Upgrading System Components)	350
Dir & Filename	javaDB.fm (ChapTitle: Directory Proxy Server)	350
Dir & Filename	serviceRegistry.fm (ChapTitle: Directory Proxy Server)	350
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	356
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	360
Dir & Filename	portalSvrSRA.fm (Head1: Multiple Instance Upgrades)	373
Dir & Filename	accessMgr.fm (Head1: Multiple Instance Upgrades)	374
Dir & Filename	accessMgr.fm (Head2: Access Manager SDK-only Upgrades).	375
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	377
Dir & Filename	directorySvr.fm (ChapTitle: Upgrading System Components)	377
Dir & Filename	webSvr.fm (ChapTitle: Upgrading System Components)	377
Dir & Filename	applicationSvr.fm (ChapTitle: Upgrading System Components)	377
Dir & Filename	accessMgr.fm (ChapTitle: Upgrading System Components)	378
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	380
Dir & Filename	directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) . . 380	
Dir & Filename	webSvr.fm (ChapTitle: Upgrading System Components)	381
Dir & Filename	applicationSvr.fm (ChapTitle: Upgrading System Components)	381
Dir & Filename	accessMgr.fm (ChapTitle: Upgrading System Components)	381
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components)	382
Dir & Filename	planning.fm (ChapTitle: Planning for Upgrades)	415
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	416
Dir & Filename	portalSvr.fm (Head3: Selective Upgrade Issues)	417
Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets)	418

Dir & Filename	planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets).	419
Dir & Filename	portalSvr.fm (Head3: Selective Upgrade Issues).	421
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	422
Dir & Filename	portalSvr.fm (ChapTitle: Upgrading System Components)	422
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	425
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	427
Dir & Filename	accessMgr.fm (Head1: Multiple Instance Upgrades)	435
Dir & Filename	accessMgr.fm (Head2: Access Manager SDK-only Upgrades).	435
Dir & Filename	accessMgr.fm (Head2: Access Manager SDK-only Upgrades).	436
Dir & Filename	accessMgr.fm (Head2: Access Manager SDK-only Upgrades).	437
Dir & Filename	accessMgr.fm (Head2: Access Manager SDK-only Upgrades).	437
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	439
Dir & Filename	directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) . 439	
Dir & Filename	accessMgr.fm (ChapTitle: Upgrading System Components).	439
Dir & Filename	portalSvr.fm (ChapTitle: Upgrading System Components)	439
Dir & Filename	sharedComps.fm (ChapTitle: Upgrading System Components).	442
Dir & Filename	directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) . 442	
Dir & Filename	accessMgr.fm (ChapTitle: Upgrading System Components).	442
Dir & Filename	portalSvr.fm (ChapTitle: Upgrading System Components)	442

