

ePolicy Orchestrator[®]

versión 3.5



McAfee[®] System Protection

Soluciones líderes de mercado en prevención de intrusiones



DERECHOS DE AUTOR

Copyright © 2004 Network Associates Technology, Inc. Todos los derechos están reservados.

Ninguna parte de esta publicación podrá ser reproducida, transmitida, transcrita, almacenada en sistema de recuperación o traducida en cualquier idioma de cualquier forma o por cualquier medio sin el permiso escrito de Network Associates Technology, Inc., de sus proveedores o de empresas afiliadas. Para obtener dicho permiso, escriba para entregar al departamento jurídico de McAfee: 5000 Headquarters Drive, Plano, Texas 75024, o llame a +1-972-963-8000.

ATRIBUCIONES DE MARCAS COMERCIALES

Active Firewall, Active Security, ActiveSecurity (y en Katakana), ActiveShield, AntiVirus Anyware y design, Clean-Up, Design ("E" Estilizado), Design ("N" Estilizado), Entercept, Enterprise SecureCast, Enterprise SecureCast (y en Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (y en Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M y Design, McAfee, McAfee (y en Katakana), McAfee y Design, McAfee.com, McAfee VirusScan, EN LA Network Associates, Net Tools, Net Tools (y en Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, VirusScan, Virusscan, Virusscan (y en Katakana), Webscan, Webshield, Webshield (y en Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. Son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo usado para denotar la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas y no registradas, mencionadas en esta publicación pertenecen exclusivamente a sus respectivos propietarios.

INFORMACIÓN DE PATENTE

Protegido por las patentes norteamericanas 6.470.384; 6.493.756; 6.496.875; 6.553.377; 6.553.378.

INFORMACIÓN DE LICENCIA

Contrato de Licencia

AVISO A TODOS LOS USUARIOS: LEA CUIDADOSAMENTE EL CONTRATO APROPIADO CORRESPONDIENTE A LA LICENCIA ADQUIRIDA, QUE ESTABLECE LOS TÉRMINOS Y LAS CONDICIONES GENERALES DE USO DEL PROGRAMA DE COMPUTADORA LICENCIADO. SI USTED NO SABE EL TIPO DE LICENCIA QUE ADQUIRIÓ, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS DE CONCESIÓN DE LICENCIA U ORDEN DE COMPRA CORRELATOS QUE ACOMPAÑAN AL EMPAQUETAMIENTO DEL PROGRAMA DE COMPUTADORA O QUE RECIBIÓ SEPARADAMENTE COMO PARTE DE LA COMPRA (COMO UNA LIBRETA, UN ARCHIVO EN EL CD DEL PRODUCTO O EN UN ARCHIVO DISPONIBLE EN EL SITIO WEB DESDE DONDE DESCARGÓ EL PAQUETE DE SOFTWARE). SI USTED NO CONCUERDA CON TODOS LOS TÉRMINOS ESTABLECIDOS EN EL CONTRATO, NO INSTALE EL PROGRAMA DE COMPUTADORA. SI PROCEDE, USTED PODRÁ DEVOLVER EL PRODUCTO A MCAFEE O A LA TIENDA DONDE LO COMPRÓ Y RECIBIR SU DINERO INTEGRALMENTE.

Atribuciones

Este producto contiene o puede contener:

- Software desarrollado por el Proyecto OpenSSL para uso en el OpenSSL Toolkit (<http://www.openssl.org/>).
- Software criptográfico escrito por Eric A. Young y software escrito por Tim J. Hudson.
- Algunos programas de computadora licenciados (o licenciados a terceros) al usuario bajo los términos de la Licencia Pública General (GPL) GNU u otras licencias semejantes de Software Libre que, entre otros derechos, permiten que el usuario copie, modifique y redistribuya ciertos programas, o partes de ellos, y tenga acceso a su código de origen. La GPL exige que, para cualquier software contemplado que sea distribuido a alguien en el formato binario ejecutable, el código de origen también sea puesto a disposición de esos usuarios. Para cualquier software de dicha naturaleza contemplada por la GPL, el código de origen está disponible en este CD. Si alguna licencia de Software Libre exige que McAfee conceda el derecho de usar, copiar o modificar un programa de computadora y dicho derecho es más amplio que los derechos concedidos en este contrato, dichos derechos prevalecerán sobre los derechos y las restricciones establecidos aquí.
- Software originalmente escrito por Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software escrito por Douglas W. Sauder.
- Software desarrollado por la Apache Software Foundation (<http://www.apache.org/>). Una copia del contrato de licencia de este software se encuentra en www.apache.org/licenses/LICENSE-2.0.txt.
- Componentes Internacionales para Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation y otros.
- Software desarrollado por CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- Tecnología FEAD® Optimizer®, Copyright Netopsystems AG, Berlín, Alemania.
- Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. y/o Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software con los derechos de autor reservados a Thai Open Source Software Center Ltd. y Clark Cooper, © 1998, 1999, 2000.
- Software con los derechos de autor reservados a los mantenedores de la Xpat.
- Software con los derechos de autor reservados a Los Regentes de la Universidad de la California, © 1989.
- Software con los derechos de autor reservados a Gunnar Ritter.
- Software con los derechos de autor reservados a Sun Microsystems®, Inc. © 2003.
- Software con los derechos de autor reservados a Gisle Aas. © 1995-2003.
- Software con los derechos de autor reservados a Michael A. Chase, © 1999-2000.
- Software con los derechos de autor reservados a Neil Winton, © 1995-1996.
- Software con los derechos de autor reservados a RSA Data Security, Inc., © 1990-1992.
- Software con los derechos de autor reservados a Sean M. Burke, © 1999, 2000.
- Software con los derechos de autor reservados a Martijn Koster, © 1995.
- Software con los derechos de autor reservados a Brad Appleton, © 1996-1999.
- Software con los derechos de autor reservados a Michael G. Schwern, © 2001.
- Software con los derechos de autor reservados a Graham Barr, © 1998.
- Software con los derechos de autor reservados a Larry Wall and Clark Cooper, © 1998-2000.
- Software con los derechos de autor reservados a Frodo Looijaard, © 1997.
- Software con los derechos de autor reservados a Python Software Foundation, Copyright © 2001, 2002, 2003. Una copia del contrato de licencia de este programa de computadora puede ser encontrada en www.python.org.
- Software con los derechos de autor reservados a Beman Dawes, © 1994-1999, 2002.
- Software escrito por Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 Universidad de Notre Dame.
- Software con los derechos de autor reservados a Simone Bordet y Marco Cravero, © 2002.
- Software con los derechos de autor reservados a Stephen Purcell, © 2001.
- Software desarrollado por el Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software con los derechos de autor reservados a International Business Machines Corporation y otros, © 1995-2003.
- Software desarrollado por la Universidad de California en Berkeley y sus colaboradores.
- Software desarrollado por Ralf S. Engelschall <rse@engelschall.com> para uso en el proyecto mod_ssl (<http://www.modssl.org/>).
- Software con los derechos de autor reservados a Kevlin Henney, © 2000-2002.
- Software con los derechos de autor reservados a Peter Dimov y Multi Media Ltd. © 2001, 2002.
- Software con los derechos de autor reservados a David Abrahams, © 2001, 2002. Véase la documentación en <http://www.boost.org/libs/bind/bind.html>.
- Software con los derechos de autor reservados a Steve Cleary, Beman Dawes, Howard Hinnant y John Maddock, © 2000.
- Software con los derechos de autor reservados a Boost.org, © 1999-2002.
- Software con los derechos de autor reservados a Nicolai M. Josuttis, © 1999.
- Software con los derechos de autor reservados a Jeremy Siek, © 1999-2001.
- Software con los derechos de autor reservados a Daryle Walker, © 2001.
- Software con los derechos de autor reservados a Chuck Allison y Jeremy Siek, © 2001, 2002.
- Software con los derechos de autor reservados a Samuel Kremp, © 2001. Consulte actualizaciones, documentación y el historial de revisiones en <http://www.boost.org>.
- Software con los derechos de autor reservados a Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software con los derechos de autor reservados a Cadenza New Zealand Ltd., © 2000.
- Software con los derechos de autor reservados a Jens Maurer, © 2000, 2001.
- Software con los derechos de autor reservados a Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- Software con los derechos de autor reservados a Ronald Garcia, © 2002.
- Software con los derechos de autor reservados a David Abrahams, Jeremy Siek y Daryle Walker, © 1999-2001.
- Software con los derechos de autor reservados a Stephen Cleary (shammah@voyager.net), © 2000.
- Software con los derechos de autor reservados a Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software con los derechos de autor reservados a Paul Moore, © 1999.
- Software con los derechos de autor reservados al Dr. John Maddock, © 1998-2002.
- Software con los derechos de autor reservados a Greg Colvin y Beman Dawes, © 1998, 1999.
- Software con los derechos de autor reservados a Peter Dimov, © 2001, 2002.
- Software con los derechos de autor reservados a Jeremy Siek y John R. Bandela, © 2001.
- Software con los derechos de autor reservados a Joerg Walter y Mathias Koch, © 2000-2002.

Índice

1	Introducción	5
	Componentes de ePolicy Orchestrator	5
	Políticas, propiedades y eventos	8
	Políticas	8
	Propiedades	8
	Eventos	8
	Tareas, servicios y cuentas	9
	Otras ocasiones en que se necesitan credenciales	10
	Requisitos mínimos	10
2	Instalación y actualización del Servidor	11
	Instalación por primera vez	11
	Preparación de la instalación	12
	Información que se debe tener a mano durante la instalación	12
	Actualización desde una versión anterior de ePolicy Orchestrator	14
	Preparación	16
	Información que se debe tener a mano durante la actualización	16
	Problemas de actualización	18
3	Organización del Directorio y de los Repositorios	19
	ePolicy Orchestrator Directory: conceptos y funciones	19
	Funciones	20
	Organización del Directorio	21
	Fronteras	22
	Filtros y clasificación de direcciones IP	23
	Repositorios	25
	Repositorios de actualización	26
	Repositorios distribuidos	27
	Repositorios del SuperAgent	27
	Métodos de actualización	28
	Actualización global	28
	Tarea de actualización del agente ePolicy Orchestrator	28
	Tareas de obtención y copia	29
4	Distribución del Agente y de los Productos	30
	Agente ePolicy Orchestrator	30
	Sobre la distribución del agente ePolicy Orchestrator	31
	Distribución del agente durante la creación del Directorio	33
	Distribución del agente tras la creación del Directorio	33
	Utilización de <i>scripts</i> de <i>login</i> para instalar el agente	33
	Instalación manual del agente	34
	Inclusión del agente en una imagen estandarizada de instalación	34
	Activación del agente en productos de McAfee sin administración	34
	Utilización de herramientas de distribución de otros proveedores para distribuir el agente	35
	Ventajas y desventajas de los métodos de distribución de agentes	35
	SuperAgents para comunicación con el servidor	36
	Sobre las llamadas de advertencia distribuidas del SuperAgent	36
	Distribución de productos con ePolicy Orchestrator	38
	Inclusión de paquetes de distribución de productos en el repositorio principal	38
	Uso de la tarea de distribución para instalar productos en clientes	40

5	Rogue System Detection	43
	Sobre el sensor Rogue Systems Detection	44
	El servidor Rogue System Detection	45
	Sobre <i>status</i> y tipos de descontrol	46
	Distribución de los sensores Rogue System Detection	47
	Distribución de sensores automáticamente por la consola	48
	Instalación manual del sensor	49
	Corrección de sistemas fuera de control	49
	Tipos de acciones	49
	Configure reacciones automáticas a eventos específicos	50
	Ejemplo de configuración de una reacción automática	50
	Marcar como Excepciones sistemas que no necesitan agentes	51
	Importación y exportación de excepciones de un archivo XML	52
6	Notificaciones de ePolicy Orchestrator	53
	¿Cómo funciona?	53
	Aceleración y agregación	54
	Reglas de notificación y las situaciones del Directorio	55
	Planificación	56
	Reglas	57
	Configuración de Notificaciones de ePolicy Orchestrator	57
	Reglas predefinidas	57
	Creación de reglas	59
	Encaminamiento de eventos	59
	Lista de productos y componentes	61
	Exhibición del historial de notificaciones	62
	Información de las notificaciones	62
	Utilización de filtros personalizados	62
7	Brotos	64
	Cosas que se deben hacer diariamente o semanalmente para permanecer listo	64
	Tareas de cliente y servidor cuya ejecución se debe programar regularmente	64
	¿Está preparado para un brote?	66
	Otros métodos de reconocimiento de brotes	66
	Principales indicadores de utilización de la red	67
	Principales indicadores de utilización <i>e-mail</i>	67
	Eventos de detección de virus	67
	¿Cree que hay un brote en curso?	68



1

Introducción

Conozca ePolicy Orchestrator 3.5

ePolicy Orchestrator 3.5 es una poderosa herramienta que permite administrar la política de seguridad, evaluar y fiscalizar políticas, identificar y tomar medidas respecto a sistemas fuera de control, y notificar sobre ciertos eventos que ocurran, en toda su red.

- *Componentes de ePolicy Orchestrator.*
- *Políticas, propiedades y eventos*
- *Tareas, servicios y cuentas*

Componentes de ePolicy Orchestrator

ePolicy Orchestrator es formado por varios componentes que se pueden instalar en sistemas de toda su red:

- *Servidor ePolicy Orchestrator.*
- *Servidor de Base de Datos.*
- *Consolas de ePolicy Orchestrator.*
- *Agente ePolicy Orchestrator.*
- *Sensor Rogue System Detection (RSD).*
- *Repositorio principal.*
- *Repositorios de actualización.*

Figura 1-1 ePolicy Orchestrator en su red

