

LinuxShield 1.3 - Actualización de la Versión

Panorama de la Versión

LinuxShield versión 1.3 es una versión intermedia que actualiza el módulo de conexión de kernel (KHM) para reconocer otros kernels de Linux que se utilizan en las varias distribuciones de Linux. Esta versión ya está disponible.

Sistemas Operativos permitidos

En esta versión de Linux 1.3 son permitidos los siguientes Sistemas Operativos:

- Red Hat 9.0
- Red Hat Enterprise 2.1 Advanced Server, Workstation, Enterprise Server
- Red Hat Enterprise 3.0 Advanced Server, Workstation, Enterprise Server
- Red Hat Enterprise 4.0 Advanced Server, Workstation, Enterprise Server, Desktop
- SuSE 8.2
- SuSE 9.0
- SuSE Enterprise 8 Server United Linux 1.0
- SuSE Linux Enterprise Server 9
- Novell Linux Desktop 9
- Novell Linux Small Business Suite 9
- Novell Open Enterprise Server 9 ejecutando Linux Enterprise Server 9 SP1

Módulos de Kernel del Linux

LinuxShield reconoce varios módulos de kernel distintos para cada distribución del Linux. La instalación de LinuxShield incluye módulos de kernel en el momento del acceso para las versiones de Red Hat y SuSE que reconocemos. Proveemos dichos módulos para las versiones del kernel original que acompañan a la distribución, y para las actualizaciones oficiales del kernel más recientes provistas por Red Hat y SuSE en el momento de esta versión.

El código fuente de los módulos de kernel también está disponible en el CD de su producto o en nuestro sitio de descargas de productos. La disponibilidad de este código fuente le permite reaccionar a parches de seguridad con la agilidad que exige su entorno específico y la política de su empresa. Sin embargo, no reconocemos módulos de kernel *personalizados* porque no podemos probarlos ni reproducir problemas específicos.

Niveles reconocidos del Kernel de SUSE

k_deflt-2.4.20-39	k_smp-2.4.19-113	k_deflt-2.4.21-99	kernel-default-2.6.5-7.97	kernel-default-2.6.5-7.111
k_smp-2.4.20-40	k_deflt-2.4.19-120	k_smp4G-2.4.21-99	kernel-smp-2.6.5-7.97	kernel-smp-2.6.5-7.111
k_deflt-2.4.20-108	k_deflt-2.4.21-198	k_smp-2.4.21-99	kernel-bigsm-2.6.5-7.97	kernel-bigsm-2.6.5-7.111
k_smp-2.4.20-108	k_smp-2.4.21-198	k_deflt-2.4.21-199	kernel-default-2.6.5-7.139	kernel-default-2.6.5-7.145
k_deflt-2.4.20-109	k_deflt-2.4.21-203	k_smp4G-2.4.21-199	kernel-smp-2.6.5-7.139	kernel-smp-2.6.5-7.145
k_smp-2.4.20-109	k_smp-2.4.21-203	k_smp-2.4.21-199	kernel-bigsm-2.6.5-7.139	kernel-bigsm-2.6.5-7.145
k_deflt-2.4.20-111	k_deflt-2.4.21-215	k_deflt-2.4.21-202	kernel-default-2.6.5-7.147	kernel-default-2.6.5-7.151
k_smp-2.4.20-111	k_smp-2.4.21-215	k_smp4G-2.4.21-202	kernel-smp-2.6.5-7.147	kernel-smp-2.6.5-7.151
		k_smp-2.4.21-202	kernel-bigsm-2.6.5-7.147	kernel-bigsm-2.6.5-7.151
k_deflt-2.4.20-113	k_deflt-2.4.21-226	k_deflt-2.4.21-215	kernel-default-2.6.5-7.151	kernel-default-2.6.5-7.191
k_smp-2.4.20-113	k_smp-2.4.21-226	k_smp4G-2.4.21-215	kernel-smp-2.6.5-7.151	kernel-smp-2.6.5-7.191
k_deflt-2.4.20-115	k_deflt-2.4.21-231	k_smp-2.4.21-215	kernel-bigsm-2.6.5-7.151	kernel-bigsm-2.6.5-7.191
k_smp-2.4.20-115	k_smp-2.4.21-231	k_deflt-2.4.21-226	kernel-default-2.6.5-7.191	kernel-default-2.6.5-7.193
k_deflt-2.4.20-120	k_deflt-2.4.21-241	k_smp4G-2.4.21-226	kernel-smp-2.6.5-7.191	kernel-smp-2.6.5-7.193
k_smp-2.4.20-120	k_smp-2.4.21-241	k_smp-2.4.21-226	kernel-bigsm-2.6.5-7.191	kernel-bigsm-2.6.5-7.193
	k_deflt-2.4.21-251	k_deflt-2.4.21-231	kernel-default-2.6.5-7.201	kernel-default-2.6.5-7.201
	k_smp-2.4.21-251	k_smp4G-2.4.21-231	kernel-smp-2.6.5-7.201	kernel-smp-2.6.5-7.201
		k_smp-2.4.21-231	kernel-bigsm-2.6.5-7.201	kernel-bigsm-2.6.5-7.201
		k_deflt-2.4.21-243		
		k_smp4G-2.4.21-243		
		k_smp-2.4.21-243		

Niveles reconocidos del Kernel de Red Hat

Red Hat 9.0	Red Hat Enterprise 2.1	Red Hat Enterprise 3.0	Red Hat Enterprise 4.0
kernel-2.4.20-8	kernel-2.4.9-e.3	kernel-2.4.21-4.EL	kernel-2.6.9-5.EL
kernel-smp-2.4.20-8	kernel-smp-2.4.9-e.3	kernel-smp-2.4.21-4.EL	kernel-smp-2.6.9-5.EL
kernel-bigmem-2.4.20-8	kernel-enterprise-2.4.9-e.3	kernel-hugemem-2.4.21-4.EL	kernel-hugemem-2.6.9-5.EL
kernel-2.4.20-30.9	kernel-2.4.9-e.12	kernel-2.4.21-9.0.1.EL	kernel-2.6.9-11.EL
kernel-smp-2.4.20-30.9	kernel-smp-2.4.9-e.12	kernel-smp-2.4.21-9.0.1.EL	kernel-smp-2.6.9-11.EL
kernel-bigmem-2.4.20-30.9	kernel-2.4.9-e.38	kernel-hugemem-2.4.21-9.0.1.EL	kernel-hugemem-2.6.9-11.EL
kernel-2.4.20-31.9	kernel-smp-2.4.9-e.38	kernel-2.4.21-9.0.3.EL	kernel-2.6.9-22.EL
kernel-smp-2.4.20-31.9	kernel-enterprise-2.4.9-e.38	kernel-smp-2.4.21-9.0.3.EL	kernel-smp-2.6.9-22.EL
kernel-bigmem-2.4.20-31.9	kernel-2.4.9-e.40	kernel-hugemem-2.4.21-9.0.3.EL	kernel-hugemem-2.6.9-22.EL
	kernel-smp-2.4.9-e.40	kernel-2.4.21-15.EL	kernel-2.6.9-22.0.1.EL
	kernel-enterprise-2.4.9-e.40	kernel-smp-2.4.21-15.EL	kernel-smp-2.6.9-22.0.1.EL
		kernel-hugemem-2.4.21-15.EL	kernel-hugemem-2.6.9-22.0.1.EL
	kernel-2.4.9-e.41	kernel-2.4.21-15.0.2.EL	
	kernel-smp-2.4.9-e.41	kernel-smp-2.4.21-15.0.2.EL	
	kernel-enterprise-2.4.9-e.41	kernel-hugemem-2.4.21-15.0.2.EL	
	kernel-2.4.9-e.43	kernel-2.4.21-15.0.3.EL	
	kernel-smp-2.4.9-e.43	kernel-smp-2.4.21-15.0.3.EL	
	kernel-enterprise-2.4.9-e.43	kernel-hugemem-2.4.21-15.0.3.EL	
	kernel-2.4.9-e.48	kernel-2.4.21-15.0.4.EL	
	kernel-smp-2.4.9-e.48	kernel-smp-2.4.21-15.0.4.EL	
	kernel-enterprise-2.4.9-e.48	kernel-hugemem-2.4.21-15.0.4.EL	
	kernel-2.4.9-e.49	kernel-2.4.21-20.EL	
	kernel-smp-2.4.9-e.49	kernel-smp-2.4.21-20.EL	
	kernel-enterprise-2.4.9-e.49	kernel-hugemem-2.4.21-20.EL	
	kernel-2.4.9-e.62	kernel-2.4.21-20.0.1.EL	
	kernel-smp-2.4.9-e.62	kernel-smp-2.4.21-20.0.1.EL	
	kernel-enterprise-2.4.9-e.62	kernel-hugemem-2.4.21-20.0.1.EL	
	kernel-2.4.9-e.65	kernel-2.4.21-27.EL	
	kernel-smp-2.4.9-e.65	kernel-smp-2.4.21-27.EL	
	kernel-enterprise-2.4.9-e.65	kernel-hugemem-2.4.21-27.EL	
		kernel-2.4.21-27.0.1.EL	
		kernel-smp-2.4.21-27.0.1.EL	
		kernel-hugemem-2.4.21-27.0.1.EL	
		kernel-2.4.21-27.0.2.EL	
		kernel-smp-2.4.21-27.0.2.EL	
		kernel-hugemem-2.4.21-27.0.2.EL	
		kernel-2.4.21-32.0.1.EL	
		kernel-smp-2.4.21-32.0.1.EL	
		kernel-hugemem-2.4.21-32.0.1.EL	
		kernel-2.4.21-37.EL	
		kernel-smp-2.4.21-37.EL	
		kernel-hugemem-2.4.21-37.EL	

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com _

McAfee y/u otras marcas mencionadas en este documento son marcas comerciales, ya sean registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color Rojo de McAfee utilizado para denotar la seguridad es una marca distintiva de los productos que llevan la marca McAfee. Todas las otras marcas comerciales, ya sean registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos titulares. (c) 2005 McAfee, Inc. Todos los derechos están reservados.