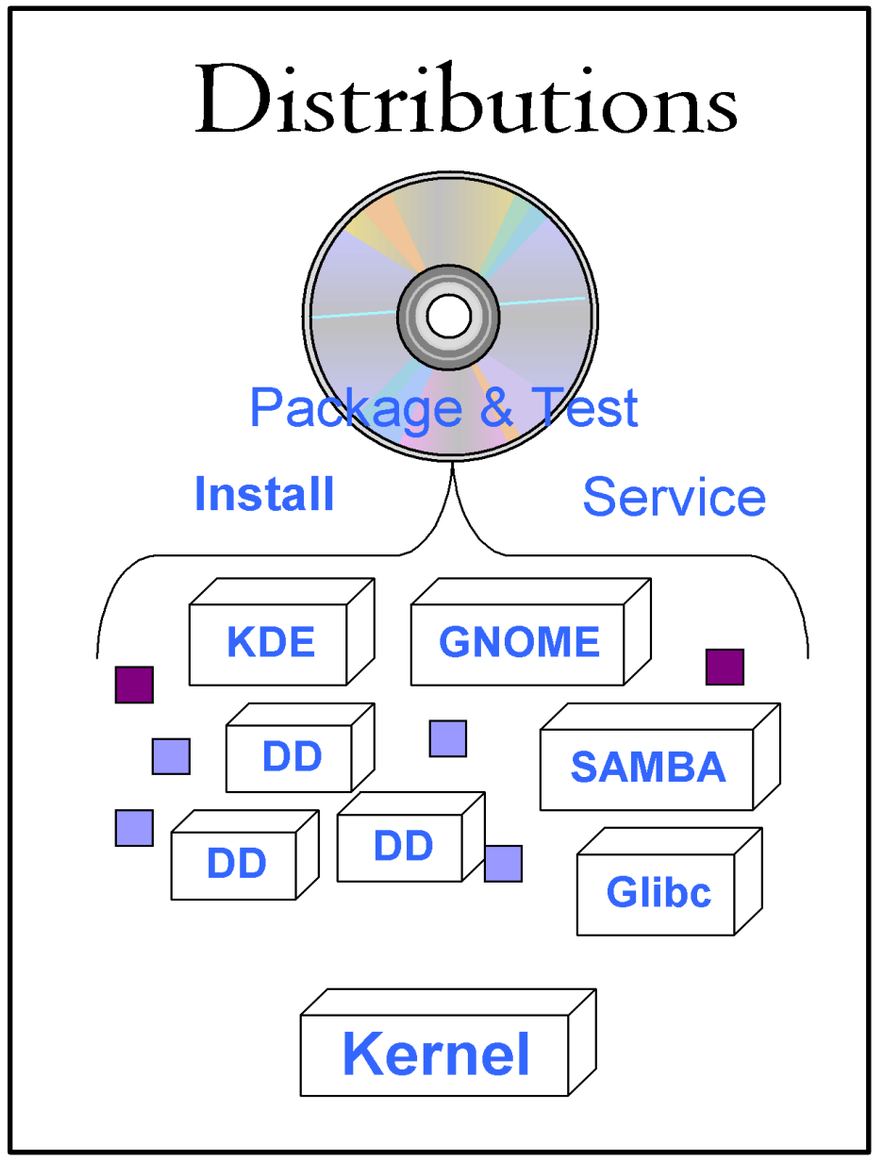
Защита информации и ОС Linux: взгляд IBM

Денис Сосновцев denis_sosnovtsev@ru.ibm.com,
Алексей Федосеев alexey_fedoseev@ru.ibm.com
Центр Компетенции Linux

Что такое Linux?

- **Свободная операционная система, разрабатываемая множеством программистов по всему миру: как волонтерами, так и при участии крупных компаний**
- **Обычно приобретается с поддержкой от создателей Дистрибутива Linux**
  - *Red Hat, SUSE / Novell, Debian*
  - *Другие, региональные дистрибутивы: Red Flag, Mandriva, Ubuntu, ...*



"Hello everybody... I'm doing a (free) operating system (just a hobby, won't be big and professional...)."

Линус Торвальдс, создатель Linux, из первого объявления в Интернет в августе 1991 года. Даже он не смог предвидеть потенциал этой системы.

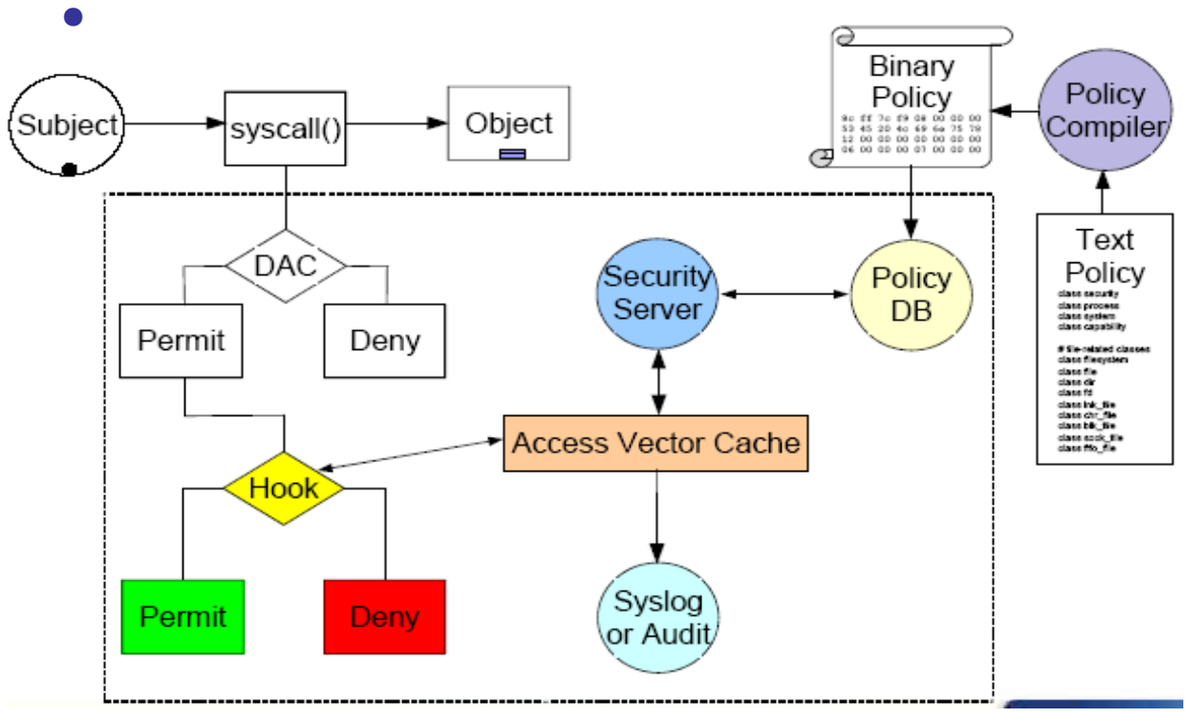
Что такое SELinux?

- **Средство повышения безопасности Linux для защиты критичной инфраструктуры**
- **Реализация мандатного метода доступа (MAC)**
- **Механизм по управлению доступом к информации со специальными метками безопасности**
- Отделение политики от исполнения
- Наиболее распространенная реализация MAC для Linux
- Поддерживает несколько механизмов доступа, в том числе многоуровневый доступ и доступ, основанный на ролях

"The goals of this project are pretty specific. We are looking to incorporate flexible mandatory access control architecture into Linux."

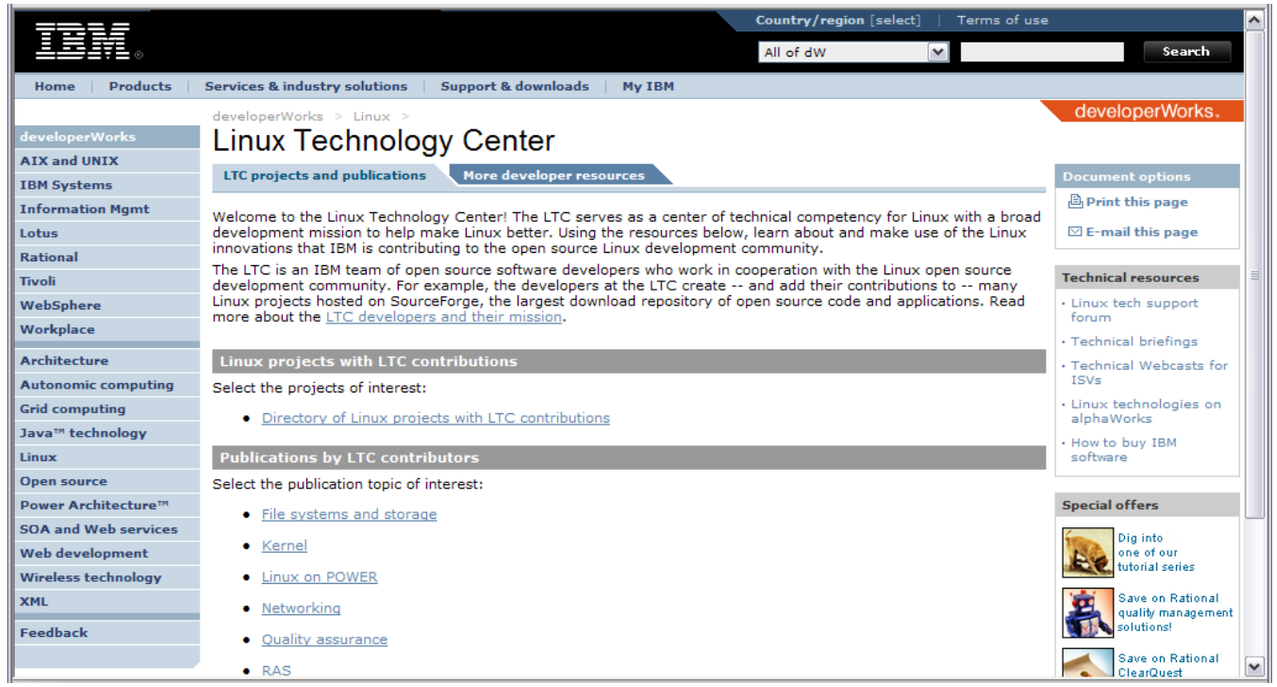
Pete Loscocco, NSA

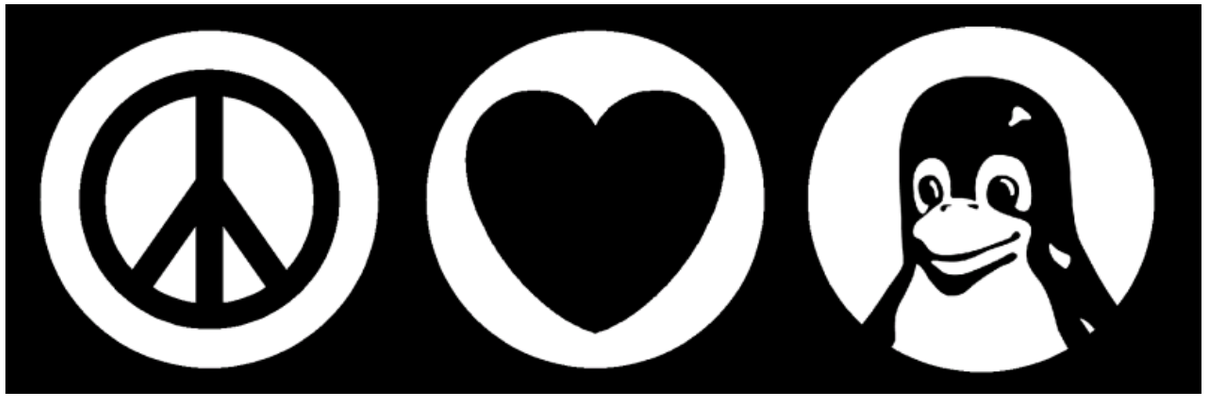
SELinux mailing list, 2001



Что такое IBM Linux Technology Center ?
(www.ibm.com/linux/ltc)

- **IBM активно участвует в разработке Linux и других сообществах разработчиков свободного ПО**
- **Команда разработчиков ОС Linux в IBM**
  - Поддержка всех аппаратных платформ IBM
  - Поддержка программных продуктов IBM
  - Другие ключевые инициативы
- **Техническая поддержка партнеров по созданию дистрибутивов Linux**
- **Техническая компетенция по серверам IBM, ПО, системам хранения и услугам в связи с Linux**





Как эти три вещи соединяются?

Разработка в сообществе

- Инфраструктура в Интернет
- Волонтеры со всего мира
- Безопасность не на первом месте

Зрелость

- Ряд IT-компаний присоединяются к сообществу
- Вывод Linux в мир бизнеса
- Улучшение безопасности

Закрепление успеха

- Индустрия IT признает роль Linux
- Все меньше компаний, не использующих OSS
- Linux зарекомендовал себя как лидер безопасных систем

1991 - 2000 | **2001 - 2005** | **2006 -**

Мизерное число анонсированных уязвимостей

Вызов Common Criteria
Можно ли сертифицировать Linux?

Бурный рост потока патчей

Защищенные вычисления (TC)

Шифрованные файловые системы

2008: IPv6

Linux 2.4

Началась разработка Flask

Новые правила США экспорта криптографии

Взлом сервера FSF

Ramen, Li0n & Adore

RHEL4 с поддержкой SELinux

OLPC объявил безопасную архитектуру

Linux версии 0.01

Stackguard

SELinux в ядре!

Аудит от Coverity

Bliss

SELinux представлен на Kernel Summit

Linux 2.6

Краткая история Linux и Common Criteria

- **Linux сертифицирован на уровни EAL2+, EAL3+, EAL4+ по профилям безопасности CAPP, LSPP и RBACPP**
- **Первая сертификация завершилась в июле 2003**
- **Несколько дистрибутивов: Red Hat и Novell**
- **Спонсоры сертификации: HP, IBM, Oracle, SGI и Unisys**
- **Linux сейчас – наиболее сертифицированная ОС**
- **Благодаря Linux LSPP-сертифицированными стало большее, чем когда-либо прежде, число аппаратных платформ**
  - Возможности масштабирования и централизации
- **Безопасность государственного уровня для массового пользователя**
  - Возможность экономить для гос. структур
  - Безопасность в стиле гос. структур теперь доступна всем
- **Проверка и оценка методологии разработки открытого ПО**
- **IBM опубликовала документы по сертификации и тестовую среду**

Deutsches IT-Sicherheitszertifikat

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0216-2003

SuSE Linux Enterprise Server V8
with certification-sles-eal2 package

from

SuSE Linux AG

sponsored by

IBM Corporation
Linux Technology Center

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0* extended by CEM supplementation "ALC_FLR – Flaw remediation", Version 1.1, February 2002 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

Functionality: **Product specific Security Target**
Common Criteria Part 2 conformant

Assurance Package: **Common Criteria Part 3 conformant**
EAL2 augmented by ALC_FLR.1 (Life cycle support - Basic flaw remediation)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the Bundesamt für Sicherheit in der Informationstechnik and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 28. July 2003

The President of the Bundesamt für Sicherheit in der Informationstechnik

Dr. Helmbrecht

IT Security Certified

SOGIS-MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 – D-53175 Bonn – Postfach 20 03 63 – D-53133 Bonn
Telefon (0228) 9582-0 – Telefax (0228) 9582-455 – Infoline (0228) 9582-111

Основные даты сертификации

Novell SUSE Linux Enterprise Server

SLES 8
(07-03)
ST / EAL2+

SLES 8 SP3
(01-04)
CAPP / EAL3+

SLES 9
(03-05)
CAPP / EAL4+

SLES 9 SP2
(10/05)
CAPP / EAL3+

SLES 10 SP1
(03/07)
CAPP / EAL4+

Jan 03 | Jan 04 | Jan 05 | Jan 06 | Jan 07 | Jan 08

ST / EAL2+
RHEL3
(02/04)

CAPP / EAL3+
RHEL3 U2
(08/04)

CAPP / EAL3+
RHEL3 U3
(09/04)

CAPP / EAL4+
RHEL4 U1
(02/06)

ОУД4+
RHEL4 U1
в ФСТЭК!

CAPP / EAL3+
RHEL4 U4
(02/07)

LSPP / RBACPP / CAPP / EAL4+
RHEL5
(06/07)

ОУД4+
RHEL4 U4
в ФСТЭК

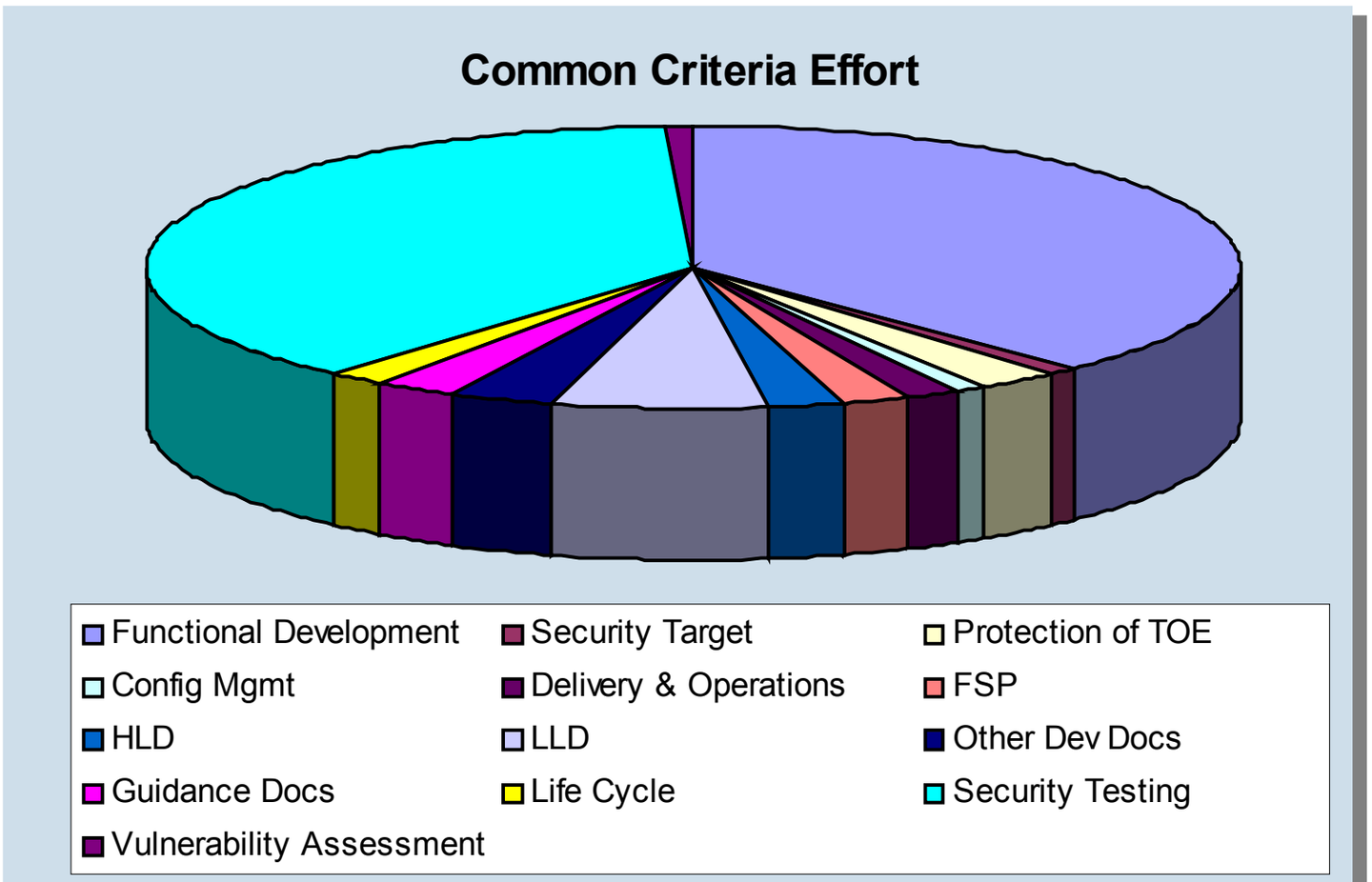
Red Hat Enterprise Linux

Чего стоила сертификация LSPP на уровень EAL4+?

“Методологически Разработана, Тестирована и Проверена”

Разработка в сообществе

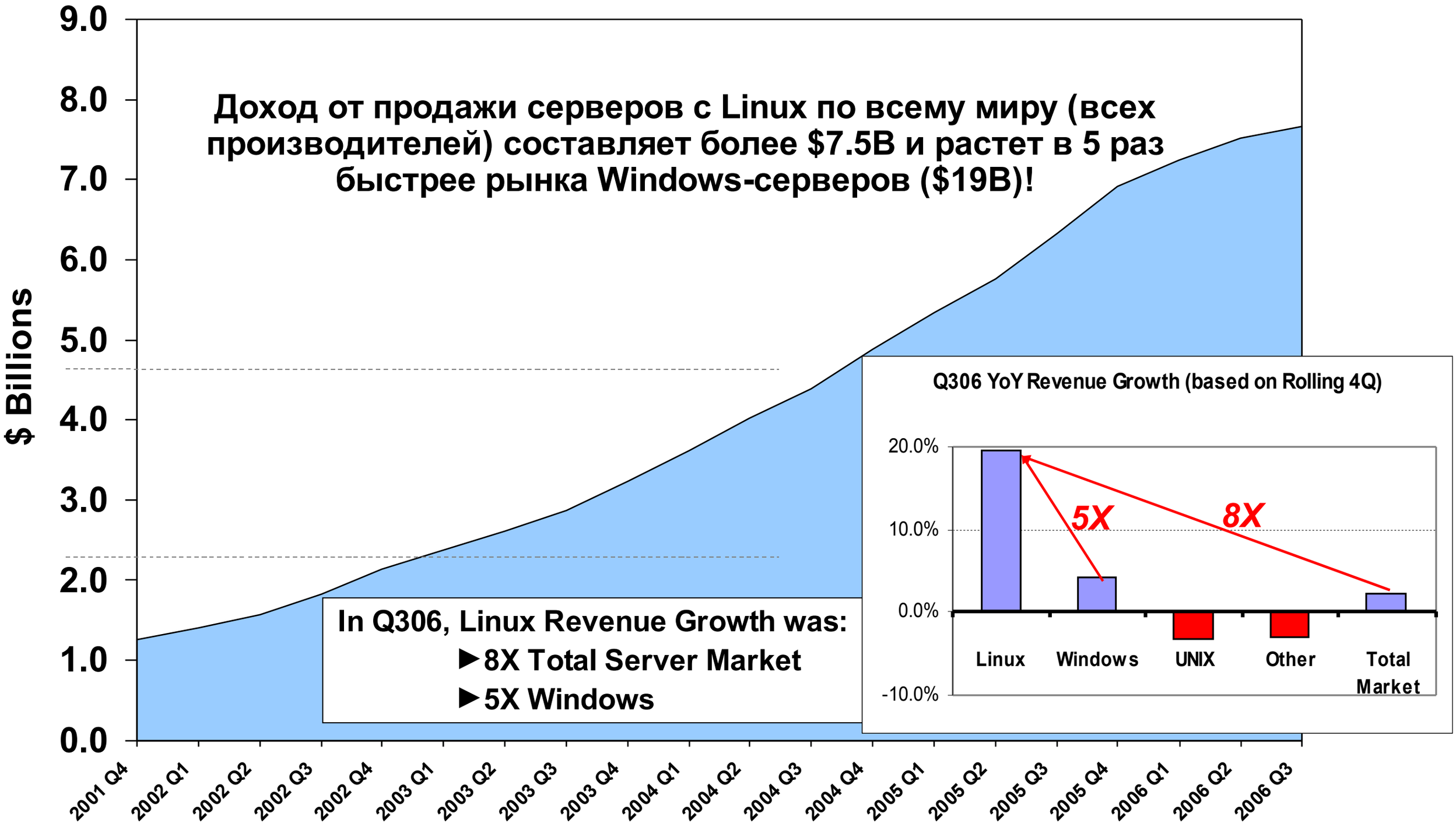
- Политика многоур. доступа
- Безопасная сеть
- Безопасная печать
- Улучшение аудита



Проверка

- Задание по безопасности : 106 страниц
- Защита функций безопасности (amtu)
- Управление конфигурацией (CVS)
- Доставка и управление: ~100 страниц
  - Руководства по установке и настройке
- Документация по разработке
  - Функц. спецификация: сотни страниц man
  - Дизайн верхнего уровня: 271 страниц
  - Дизайн низкого уровня: ~ 800 страниц
  - Модель политики безопасности: 11 страниц
- Сопровождающая документация: ~825 страниц
  - Руководство пользователя и администратора безопасности
- Жизненный цикл
  - Процесс создания патчей и обновления
- Тестирование
  - План тестирования
  - 1200 тестовых ситуаций
- Проверка уязвимостей: ~ 50 страниц

Рынок серверов нуждается в Linux и (все еще) растет!



Source: Gartner Quarterly Statistics Rolling 4 Quarters 3Q06

Linux: Правительство Великобритании

Цель

- Создать пилот защищенной ОС Linux, который позволили бы осуществить доступ к данным между департаментами “когда угодно и откуда угодно”, обеспечив доверенную инфраструктуру для служб и приложений на основе преимущественно WebSphere и DB2.

Ключевые преимущества*

- Ограничение и защита процессов на сервере (sandboxing)
- Многоуровневая безопасная архитектура
- Защита от проникновений

Решение

- Tresys разрабатывает и тестирует политику (11/05 - 05/06)
- IBM тестирует пилот (05/06 - 07/06)
- Belmin тестирует интеграцию пилота (07/06 - 08/06)
- Использование пилота (в режиме разрешения) (08/06 - 10/06)
- **Работа в нормальном режиме** (11/06)

* http://www.computerwire.com/industries/research/?pid=1C0B88FA-A04B-4A0E-862F-D51D898CBBC9

Linux: Морская пограничная служба США

United States Coast Guard
U.S. Department of Homeland Security

Цель

- Создать безопасную среду Linux, позволяющую пользователям осуществлять работу в нескольких независимых сессиях с разными уровнями доступа.

Ключевые преимущества*

- Решение с открытым кодом, которое дает недорогую альтернативу закрытым проприетарным решениям
- Предотвращение взаимного проникновения и заражения
- **Уменьшенный риск и Совокупная стоимость владения**

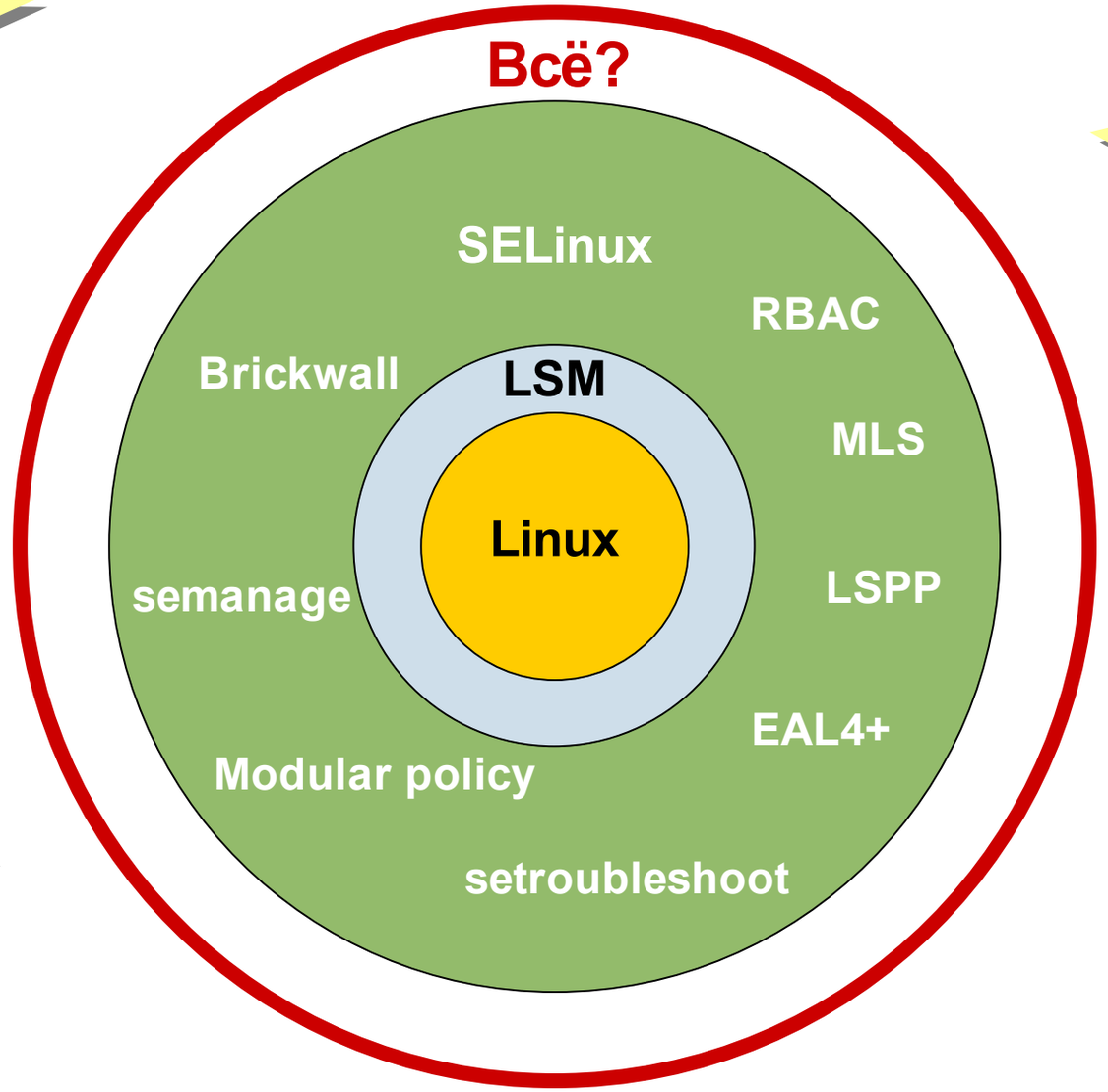
Решение

- Тонкий клиент TCS NetTop2
- SELinux –IBM Linux Technology Center, совместно с Red Hat, TCS и сообществом разработчиков Linux
- IBM System x

* http://www.trustedcs.com/news/6news6_1_2j.htm

SELinux сегодня: этап использования и улучшения

Избежать проблем от взломанных программ



Уточнить доступ и права пользователей

Уйти от зависимости от суперпользователя

Ограничить привилегии пользователей и приложений

Все больше примеров использования в гос. секторе

SELinux завтра

Рынок SMB / Простота

Широкое распространение

Интеграция между ОС

Стандартизация

Управление из коробки

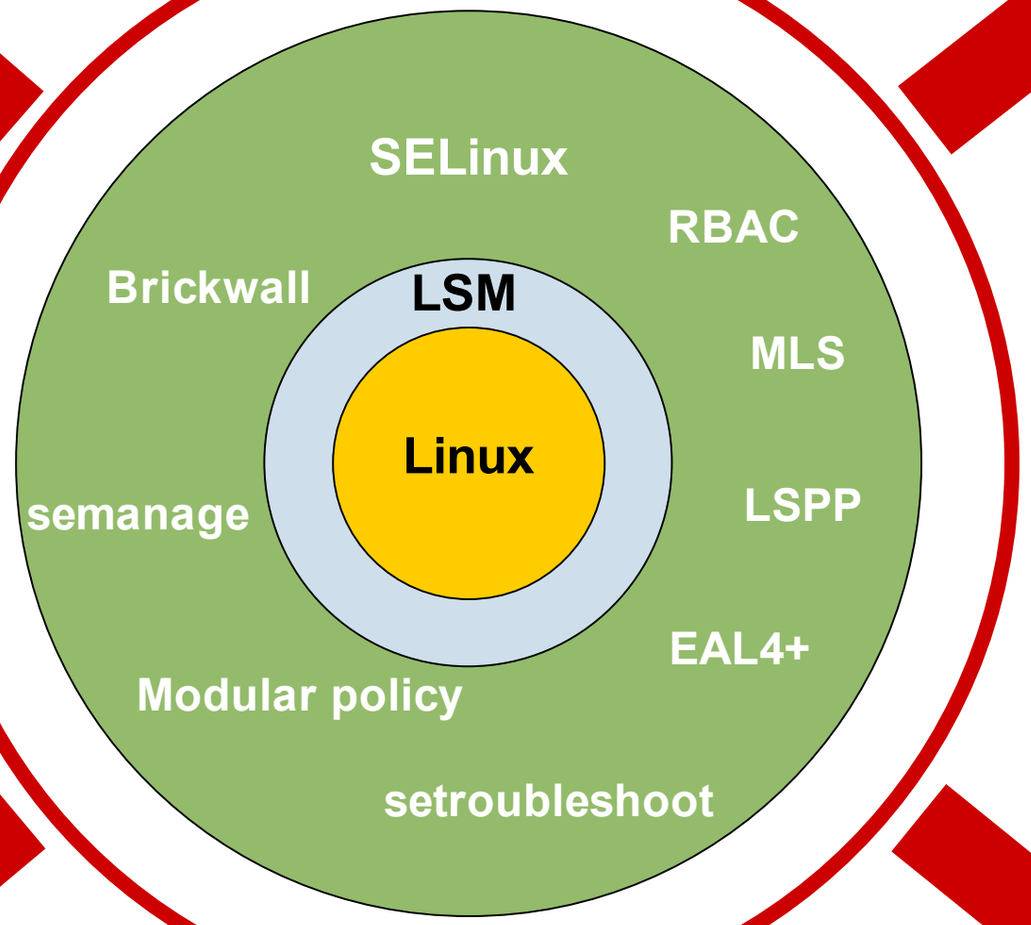
“Как это отключить?”

Политики для ISV

Централизов анное упр. политикой

Примеры политик

Всё? НЕТ!



Интеграция в БД

Real-Time + SELinux

Безопасность приложений

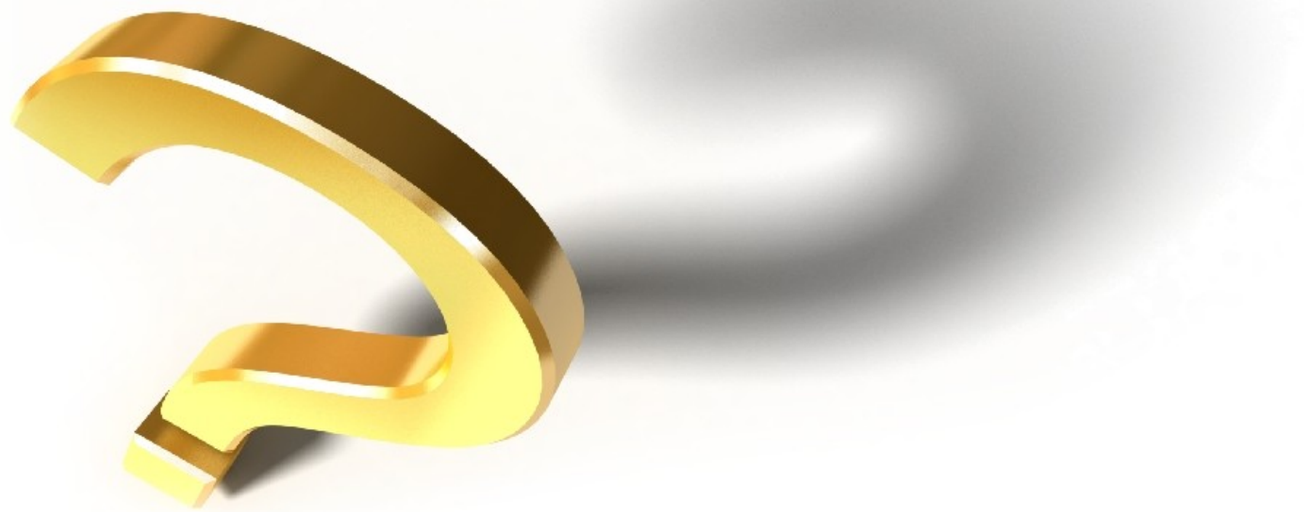
Защищенный X Windows

Обязательное шифрование

Технологии

Спасибо!

. . . Вопросы?



Trademarks and Presentation Notes

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: eServer, System x, System p, System i, System z, IBM.

The following are trademarks or registered trademarks of other companies:
Java and all Java based trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries or both
Microsoft, Windows,Windows NT and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.
Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
Red Hat, Red Hat Linux are registered trademarks of Red Hat, Inc.
SUSE is a registered trademark of Novell, Inc.
Other company, product, or service names may be trademarks or service marks of others.

Any statements about support or other commitments may be changed or cancelled at any time without notice. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only Information is provided "AS IS" without warranty of any kind.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM makes no representation or warranty regarding third-party products or services including those designated as ServerProven, ClusterProven or BladeCenter Interoperability Program products. Support for these third-party (non-IBM) products is provided by non-IBM Manufacturers.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.