

# EAL4+ bezpieczeństwo z SUSE Linux Enterprise Server

---

Dariusz Leonarski  
Novell Polska  
dleonarski@novell.pl



**Novell**®



# Agenda

---

- „Common Criteria”
- SLES w zastosowaniach profesjonalnych
- Bezpieczeństwo w SUSE
- Novell AppArmor
- Pokaz AppArmor

# Common Criteria

---

- międzynarodowy standard ISO 15408 dla bezpieczeństwa komputerowego
- cele:
  - umożliwienie specyfikowania przez użytkowników wymagań dotyczących bezpieczeństwa
  - umożliwienie specyfikacji atrybutów bezpieczeństwa ich produktów
  - umożliwienie testerom sprawdzenie, czy produkt spełnia wymagania dotyczące bezpieczeństwa
- EAL (Evaluation Assurance Levels) - predefiniowany zestaw wymagań dotyczących bezpieczeństwa - poziomy od 1 do 7

# EAL - Level 1

---

## Testy funkcjonalne:

- wykorzystywany w systemach, gdzie poufność jest wymagana do poprawnej pracy, ale zagrożenia bezpieczeństwa nie są traktowane całkiem poważnie
- testy na tym poziomie powinny dostarczyć dowodów na to, że testowany system jest zgodny z dokumentacją i posiada skuteczną ochronę przed zidentyfikowanymi problemami
- wykorzystywany do ochrony prywatnych informacji

## EAL - Level 4

---

Zaprojektowany, testowany i prezentowany zgodnie z metodologią:

- analizy na niskim poziomie projektowania systemu
- analizy wykonywane na wycinkach implementacji
- testowanie przez niezależne osoby w poszukiwaniu błędów
- wspomaganie przez zarządzanie modelem „cyklu życia”

# SLES w zastosowaniach profesjonalnych

---

- bazy danych - Oracle, DB2
- serwer plików - NFS, Samba
- serwer WWW - Apache
- serwer poczty - Postfix + Cyrus
- serwer FTP
- zewnętrzne rozwiązania - eDirectory, GroupWise, Lotus Notes
- klastry PolyServe



# Najlepszy wynik testu wydajnościowego TPC-C

## „Oracle uzyskał rekordową wydajność bazy danych wykorzystując SUSE LINUX Enterprise Server 9”

- Serwer NEC Express 5800/1320Xd z 32 procesorami Intel Itanium 2 1.5 GHz, 6 MB L3 cache z systemem **Novell's SUSE LINUX Enterprise Server 9**, Oracle 10g osiągnął wynik 683,575 tpmC (transactions per minute) ze stosunkiem ceny do wydajności \$5.99/tpmC.
- Test wydajnościowy TPC-C dla bazy Oracle 10g na linuxowych systemach wieloprocessorowych (SMP)
- <http://www3.sys-con.com/banners/linuxworld336.cfm>

"More and more customers are turning to Linux to support their large-scale enterprises. By showing outstanding Linux database performance on the largest SMPs, Oracle continues to prove that Linux can handle the world's toughest workloads."

- Richard Sarwal, vice president of Server Performance of Oracle Corp.



# Carrier Grade Linux, Data Center Linux

---

SUSE LINUX pierwszy system linuksowy klasy przemysłowej zgodny z *Carrier Grade Linux*

- [http://www.osdl.org/lab\\_activities/carrier\\_grade\\_linux/](http://www.osdl.org/lab_activities/carrier_grade_linux/)
- Standard przemysłowy, wywodzący się z zastosowań komunikacyjnych, ale stosowany (wymagany) znacznie szerzej
- Korzyści nie tylko w dziedzinie komunikacji

Wiele wymagań wspólnych z *Data Center Linux*

- Stabilność, nieprzerwana dostępność, użyteczność (RAS)
  - Mechanizm Crash Dump i szybki restart
  - Sieciowa konsola administratora
- Zarządzanie wolumenami klastrowymi
  - Intuicyjna konsola administratora EVMS

# Bezpieczeństwo w SuSE

**Problem:** Jak zapewnić poufność danych i umożliwić administratorowi ich odpowiednie zabezpieczenie?

**Rozwiązanie:** SUSE LINUX Enterprise Server umożliwia wysoki, potwierdzony certyfikatami poziom zabezpieczenia danych i całej sieci



## Cechy

- Wirtualne sieci prywatne
- Certyfikat bezpieczeństwa EAL
- Zarządzanie certyfikatami
- Wsparcie szyfrowanych systemów plików
- Zabezpieczenia połączeń sieciowych

# Wbudowane systemy zabezpieczeń

---

Wirtualne sieci prywatne (VPN)

Kontrola dostępu do zasobów (ACL)

Bezpieczne połączenia z wykorzystaniem 128-bit  
SSL, IPsec, Secure Shell, Kerberos 5 itp.



Zarządzanie certyfikatami

Wbudowane monitorowanie

- Operacje na plikach
- Wykrywanie intruzów
- Linux Audit System (LAuS)

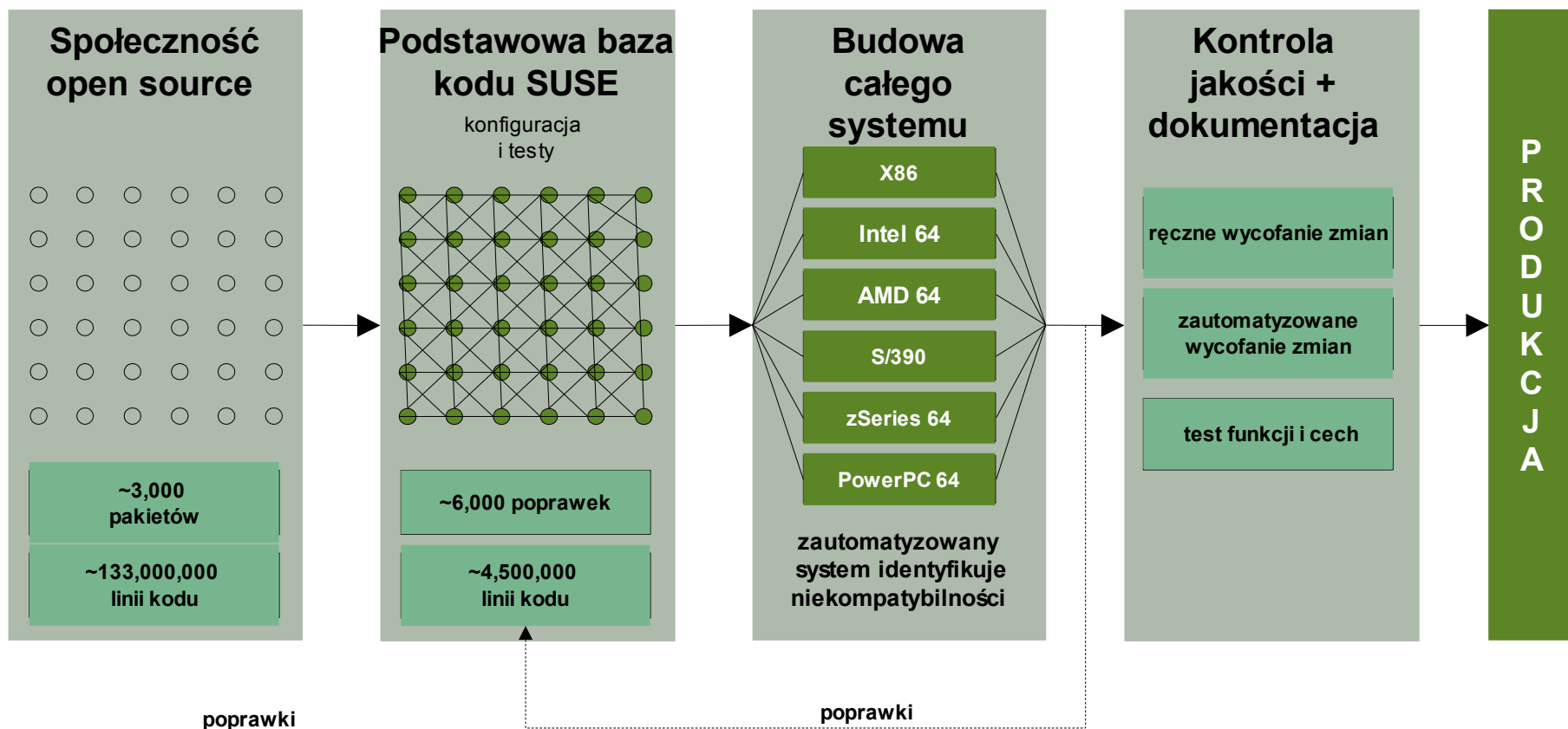
Wsparcie dla szyfrowanych systemów plików

SUSE LINUX Firewall and Proxy Suite

- Konfiguracja reguł zabezpieczeń, NAT itp.

# Bezpieczeństwo w SUSE - produkcja

- wspólne repozytorium dla wielu wersji architektur





# Bezpieczeństwo w SUSE - produkcja

- intensywne testowanie przed wydaniem wersji produkcyjnej - openSUSE, Novell Linux Desktop, SUSE Linux Enterprise Server
- ~ 6 000 000 linijek poprawek nałożonych na system
- łatki na wszelkie dziury aplikowane są na wszystkie wersje/odmiany systemu
- bardzo szybka reakcja na błędy - łatki dystrybuowane poprzez OnlineUpdate lub RedCarpet
- „własne” poprawki do jądra

# W efekcie, od 9 III 2005 mamy ...




Новости - Linux General - SuSE Linux получил сертификат EAL4 - Mozilla Firefox

Плнк Едycja Widok Przejdz Zakladki Narzедzia Pomoc

http://www.linux.org.ru/view-message.jsp?msgid=811797

SUSE LINUX Entertainment News Internet Search Reference Maps and Directions Shopping

 **LINUX.ORG.RU** Новости - Галерея - Форум - Документация - Поиск

<a href="#">&lt;&lt;&lt;</a> Европарламент отклонил закон о патентах на ПО (Коммерческое ПО)	<a href="#">Новости - Linux General</a>	Викимедиа нуждается в вашей помощи <a href="#">&gt;&gt;&gt;</a> (OpenSource)
---	---	---

## SuSE Linux получил сертификат EAL4

### SuSE Linux получил сертификат EAL4

SuSE Linux Enterprise Server 9 получил сертификат по Common Criteria EAL4+. На данный момент SLES9 является первым дистрибутивом Linux который был сертифицирован по этой программе.

Теперь SLES9 находится в одной лиге с такими игроками как Microsoft (Windows 2000) на рынке систем для правительства.

Novell.

# Novell AppArmor

---



Novell®



# Co to jest AppArmor?

---


AppArmor jest produktem wprowadzającym mechanizm ACL do jądra systemu Linux.

- duża szybkość działania
- łatwy w modyfikowaniu plik profilu
- dobra integracja z systemem poprzez LSM - nie ingeruje bezpośrednio w kod jądra
- bardzo małe straty wydajności - w większości testów w zakresie błędu pomiaru


# AppArmor vs inne rozwiązania


	AppArmor	GRSecurity	SELinux
Licencja	Komercyjna	GPL	GPL
Możliwości	ACL	ACL + wiele dodatkowych zabezpieczeń	rozbudowane ACL
Łatwość konfiguracji	bardzo łatwa	od łatwej do średniej	trudna
Integracja	moduł LSM	łatka na kernel	łatka na kernel
Szybkość	w granicach błędu pomiarowego	zależnie od konfiguracji od kilku do kilkunastu %	zależnie od konfiguracji do kilkunastu %
“Profiler”	TAK	NIE	NIE


# Zródła informacji

 **suse eal4+ - Szukaj w Google - Mozilla Firefox**

Plik Edycja Widok Przejdź Zakładki Narzędzia Pomoc





 [WWW](#) [Grafika](#) [Grupy dyskusyjne](#) Nowość! [Katalog](#)

Szukaj w Internecie  Szukaj na stronach kategori

---

**WWW** Wyniki 1 - 10 spośród około 16,600 dla zapy

[EAL4+ for Suse Linux \(Linux\)](#)  
How many Open Source apps does it take to screw in a light bulb? Here's the la  
word from the Linux galaxy, Open Source projects, command line assistance ...  
[channels.lockergnome.com/linux/archives/20050221\\_eal4\\_for\\_suse\\_linux.phtml](http://channels.lockergnome.com/linux/archives/20050221_eal4_for_suse_linux.phtml)

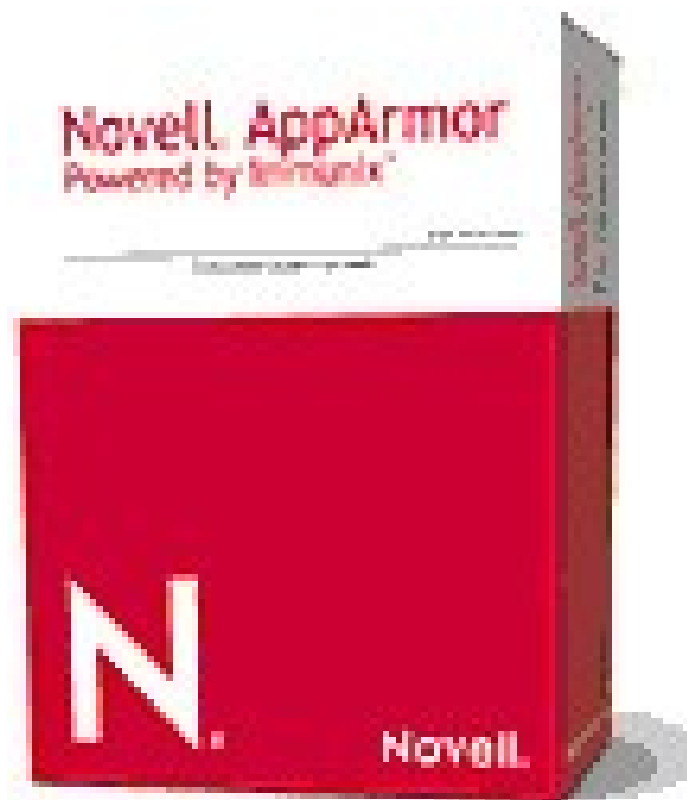
[Atsec Completes CAPP/EAL4+ Security Evaluation for SUSE Linux ..](#)  
Atsec information security has completed a Common Criteria evaluation of Novel

- Common Criteria
  - <http://www.commoncriteriaportal.org/>
  - <http://www.commoncriteriaportal.org/public/expert/index.php?menu=7>
  - [http://en.wikipedia.org/wiki/Evaluation\\_Assurance\\_Level](http://en.wikipedia.org/wiki/Evaluation_Assurance_Level)
- Wskazówki konfiguracyjne dla SuSE
  - <http://www.uniform.chi.il.us/slides/HardeningLinux/IBM-SLES-EAL4-Configuration-Guide.pdf>
- No i zawsze :-)
  - <http://www.novell.com>



# Zapraszam na pokaz AppArmor

---



Novell.

Novell.®