Megerősített hátország a Novell SUSE Linux Enterprise Serverrel

Ha az informatikai életben a nagyobb teljesítményről, jobb méretezhetőségről, felügyelhetőségről, megbízhatóságról, nagyobb biztonságról, jobb támogatásról beszélünk és a vállalatokat erről az oldalról közelítjük meg, a Novellt az elsők között kell említenünk.

A vállalat legújabb termékcsaládja, a ***SUSE Linux Enterprise 10*** a cégek számára sokkal többet kínál a világszínvonalú vállalati szerveroperációs rendszerektől elvárt funkciókból. Mint minden új kiadás esetén, a platform kiszolgálókomponense, a ***SUSE Linux Enterprise Server*** természetesen több funkcióval rendelkezik mint elődje, azonban a kiszolgáló három lényeges bővítése az, amitől a szerver nagyot lép előre az egyre nagyobb igényt támasztó vásárlók szemében.

- *AppArmor* alkalmazásbiztonság
- Tárolási alapok
- A kiszolgálók virtualizációja

Az AppArmor megerősített alkalmazásbiztonságot nyújt

A biztonság mindig is a *Linux* operációs rendszer egyik erőssége volt, de az egyes alkalmazások sérülékenysége néha kaput nyit a betörők előtt. A ***SUSE Linux Enterprise*** termékcsaládba teljes mértékben integrált *AppArmor* alkalmazásbiztonsági keretrendszer segít e probléma megoldásában, mivel egy speciális biztonsági csomagolást készít minden egyes alkalmazás köré.

Az *AppArmor* nem teljesen új a ***SUSE Linux Enterprise Server*** felhasználói számára. A korábbi, 9-es verzió ugyanis már tartalmazott egy nyílt forráskódú kernelmodult és egy biztonsági egyeztetést kezelő komponenst, azonban az irányelvek létrehozásának és értelmezésének lehetősége külön, még egyedi megoldásként volt kapható. Az *AppArmor* mostanra teljesen nyílt forráskódúvá vált (a ***GNU General Public License*** szerint) és szorosan integrálódik a ***SUSE Linux Enterprise*** keretrendszerbe.

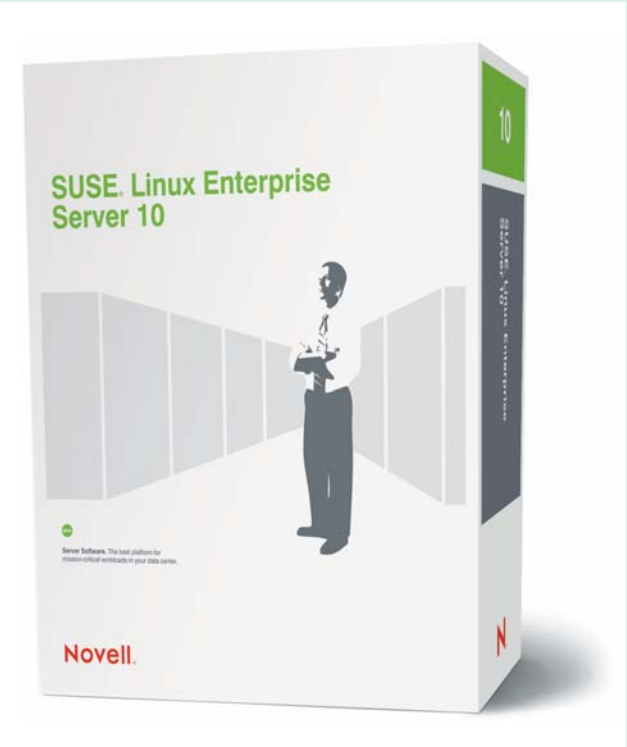
Az *AppArmor* a vállalati alkalmazások védelmére egy „fehérlista” elvet alkalmaz, ahol fel van tüntetve, hogy az alkalmazások milyen műveletek végrehajtására jogosultak. Ez a módszer sokkal hatékonyabb a „feketelistás” módszereknél, ahol az van felsorolva, hogy az alkalmazásnak mit *nem* szabad csinálnia. A feketelistás módszerek ugyanis csak addig működnek biztonságosan, amíg új támadási pontok nem válnak ismertté. Ilyenkor a felhasználók védtelenek, ameddig a gyártók el nem készítik az új javításokat.

Az irányelvek – a gyakorlatban egyszerű szövegfájlok – létrehozásuk után egyszerűen szétoszthatók a környezet más olyan kiszolgálóira, amelyek ugyanazokat az alkalmazásokat futtatják és ugyanazokat az irányelveket igénylik. Az *AppArmor* frissítésiprofilkészítő varázslójával egyszerűen frissíthetők a meglévő alkalmazás-irányelvek, vagyis könnyen implementálhatók a változások és vehetők fel az új szabályok. Miután az alkalmazás-irányelv életbe lépett, az *AppArmor* naplózza az irányelv által visszautasított alkalmazáseseményeket. A profilkészítő varázslóhoz hasonlóan a frissítésiprofil-készítő varázsló is átnézi a naplót és kérdéseket tesz fel oly módon, hogy könnyen ki tudja egészíteni a meglévő irányelvet.

A felügyelhetőség terén újdonság a ***Novell Customer Center*** (ügyfélközpont), ahol egyszerűen kezelhetők a rendszer-előfizetések. A ***Customer Center*** egy központi online portál, ahol a műszaki támogatás mellett a szoftverfrissítések, hibajavítások is egy helyen elérhetőek, és amely teljes mértékben együttműködik a ***Novell ZENworks® Linux Managementtel***. A ***Novell ZENworks Linux Management*** segít a ***Linux*** kiszolgálók és asztali gépek felügyeletében, így egészen nagy felhasználói bázis is kezelhető, és szabályozható a hozzáférés a hálózatokhoz és alkalmazásokhoz az ***OpenLDAP*** segítségével. A ***SUSE Linux Enterprise Server*** maximálisan integrálható Novell eDirectory környezetekbe, de ***Active Directory*** infrastruktúrákba is.

Robusztusabb, jobban méretezhető és nagyobb rendelkezésre állású tárolóeszközök

A ***SUSE Linux Enterprise Serverben*** található új tárolóeszköz-kezelő alaprendszer most többet nyújt, hiszen robusztusabb és jobban kezelhető



alapot biztosít, amely képes kiszolgálni kis fájlrendszereket, vagy akár fájlok millióit több terabájtnyi tárterületen. Emellett alkalmazások széles körét is kiszolgálja a webes alkalmazásoktól kezdve egészen az adatbázisokig, és a korábbiaknál nagyobb rendelkezésre állást garantál a továbbfejlesztett clusterkezelési funkciókkal és a speciális cluster-fájlrendszerrel.

Virtuálisan még több kiszolgáló

A ***SUSE Linux Enterprise Server*** disztribúció talán legizgalmasabb újdonsága a kiszolgálóvirtualizáció lehetősége. A ***Cambridge Egyetem*** által működtetett ***Xen*** nyílt forráskódú projektre épülő kiszolgálóvirtualizáció segít abban, hogy az alkalmazásokat, szolgáltatásokat és fájlrendszereket ne kelljen egy-egy adott géphez rendelni.

A virtualizáció előnye igazán akkor látszik, ha több önálló virtuális gép is fut egyetlen fizikai kiszolgálón. Ez lehetővé teszi a terhelések elszigetelését, vagyis ahelyett, hogy több alkalmazás futna ugyanazon a „túlhizlalt" operációs rendszeren, az egyes alkalmazások elszigetelhetők és a saját virtuális gépen futtathatók. Ha egy alkalmazás lefagy, – mivel el van szigetelve –, egyáltalán nem befolyásolja a többi szolgáltatást és alkalmazást, amelyek a saját virtuális gépeiken belül futnak ugyanazon a kiszolgálón. Ha egy virtuális gépen csak egyetlen alkalmazás vagy szolgáltatás fut, elegendő csupán az operációs rendszernek azokat a szolgáltatásait és komponenseit betölteni, amelyekre az alkalmazásnak ténylegesen szüksége van.

Így a fejlesztők és integrátorok számára lehetőség nyílik arra, hogy speciális virtuális gépeket készítsenek megoldásaikhoz.

A kiszolgáló virtualizációja újabb szintet ad hozzá a magas rendelkezésre álláshoz: a meghibásodott szolgáltatás automatikus újraindítását. Ez azt jelenti, hogy az alkalmazás vagy szolgáltatás csak egy rövid időre áll le, általában nem elég hosszú ideig ahhoz, hogy komoly problémát jelentsen.

A ***Virtual Machine Migration*** (virtuális gép áthelyezése) funkció lehetővé teszi egy adott virtuális gépen futó alkalmazás vagy szolgáltatás áthelyezését az egyik fizikai gépről a cluster egy másik gépére, újraindítás nélkül. Ez azt jelenti, hogy nincs leállás és az alkalmazás futási állapota teljesen megőrzésre kerül áthelyezés közben. Ez nagy előny, mert így éles működés közben is elvégezhető a rendszer normál karbantartása.

Ha a kiszolgálók konszolidációjáról van szó, a több virtuális gép futtatása egyetlen kiszolgálón, valamint az a tény, hogy a virtuális gépek akár más-más vendég operációs rendszereket is futtathatnak, nagymértékben megkönnyítheti a felhasználók dolgát. Legyen bár a ***SUSE Linux Enterprise Server*** a gazda operációs rendszer a kiszolgálóvirtualizációhoz, a virtuális gépek maguk más paravirtualizált vendég operációs rendszereket is futtathatnak. (A paravirtualizáció egy olyan virtualizációs megoldás, ahol a hardverhez nagyon hasonló, bár azzal nem teljesen megegyező szoftverfelületet „látnak" a virtuális gépek.) Vagyis az olyan meglévő alkalmazások, amelyeknek muszáj egy adott régebbi operációs rendszeren futni, elszigetelhetők a saját egyéni virtuális gépükbe, ugyanakkor mégis futhatnak ugyanazon a fizikai kiszolgálón. A ***SUSE Linux Enterprise Server*** az ***AMD*** és az ***Intel*** hamarosan elkészülő hardvertechnológiáival együtt képes lesz támogatni a teljes virtualizációt.

A ***SUSE Linux Enterprise Server*** teljesen virtualizált és paravirtualizált vendég operációs rendszer támogatást is biztosít. A ***Novell*** még ebben az évben tervezi a paravirtualizációs támogatást a ***SUSE Linux Enterprise Server 9 SP3***-hoz, valamint az ***Open Enterprise Server*** környezetben futó ***NetWare*** támogatását.

A hivatalosan bejelentett támogatásokon túl, a nyílt forráskódú közösségnek a ***Xenen*** paravirtualizált vendég operációs rendszerként futó kernelek között megtalálható a ***Linux 2.4***, a ***Linux 2.6***, a ***NetWare 6.5***, a ***NetBSD***, a ***FreeBSD***, a ***Plan9*** és az ***OpenSolaris***. Bár a vendég operációs rendszerek bejelentett támogatása egyelőre korlátozott, a ***Novell*** célja, hogy a ***SUSE Linux Enterprise Serveren*** futó ***Xen*** legyen a kapható legjobb virtualizációs platform. A jövőben tehát további újdonságokra számíthatunk még.

AppArmor-közösség

Annak érdekében, hogy még egyszerűbb legyen minden szervezet számára az ***AppArmor*** kínálta alkalmazásbiztonsági előnyök kiaknázása, a ***Novell*** meghirdetett egy nyílt forráskódú projektet, ahová mindenkit szívesen vár, hogy járuljon hozzá az AppArmor jövőbeni fejlesztéséhez, valamint küldjön el a saját alkalmazásaihoz készített ***AppArmor*** profilokat. A cél előredefiniált alkalmazásbiztonsági irányelvek nagy tárházának kialakítása, amely mindenkinek segíthet az ***AppArmor*** gyors és egyszerű beüzemelésében az informatikai környezetek védelméhez. További információ a projekttel kapcsolatban: ➲ opensuse.org/apparmor.