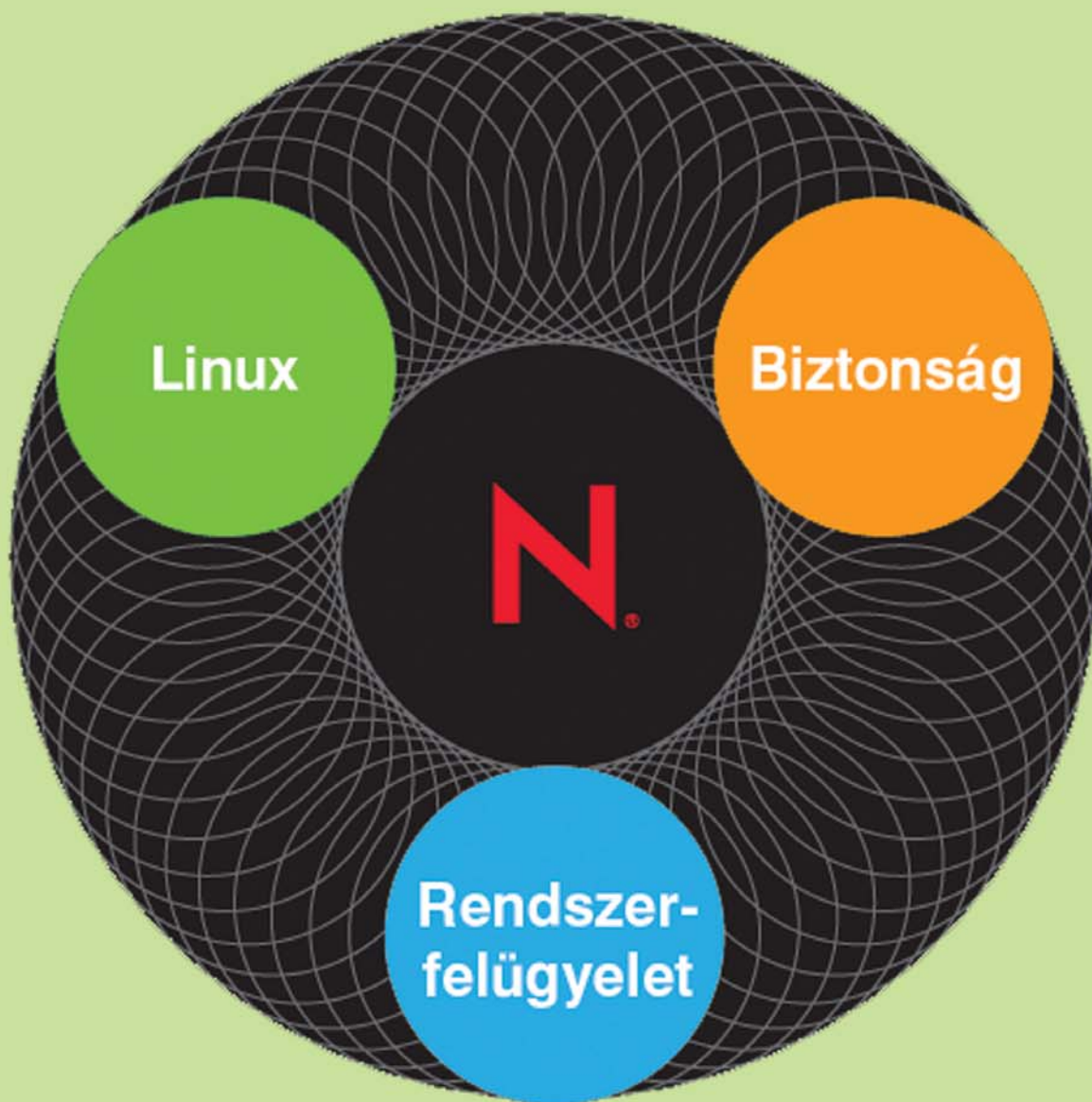


Connection

Novell Connection Magazin
VIII. ÉVFOLYAM SZEPTEMBER/2008



Az új Novell:
Linux, Biztonság, Rendszerfelügyelet

Novell.



Informatikai rendszerfejlesztésének következő állomása: A jogosultságok központosított felügyelete A Novell Identity Managerrel

Azonnal megtérülő beruházás, amely tökéletes hozzáférést és teljeskörű védelmet biztosít

- ➔ Lehetővé teszi a biztonságos, személyazonosságokon alapuló hozzáférések kialakítását
- ➔ Megszünteti a felhasználó- és jogosultságkezelési valamint hozzáférési anomáliákat
- ➔ Automatizálja a jogosultság igénylés és jóváhagyás folyamatát és teljes körű naplózást biztosít hozzá
- ➔ Az alkalmazottak így csak ahhoz férhetnek hozzá, amihez jogosultságuk van,
a munkájukhoz szükséges adatokat viszont bárholnan, bármikor, biztonságosan elérhetik

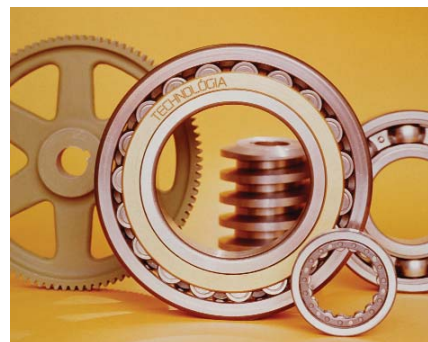
Dőljön hátra, mert biztos lehet abban, hogy bizalmas adatai tökéletes védelmet kapnak!





8

12



22

Beköszöntő

Mindannyiunk számára elengedhetetlen a piaci igények változásának folyamatos követése. Így tett a Novell is az elmúlt években, amikor a kialakított stratégiai területeken saját kompetenciáját számos felvásárlással és piacvezető, innovatív technológiák integrálásával egészítette ki: a Novell mára a vállalati szoftvermegoldások egyik vezető szállítójává vált. Világszerte vezető szerepet töltünk be a Linux-alapú és nyílt forráskódú vállalati operációs rendszerek, valamint a vegyes forráskódú, heterogén informatikai környezetek működtetéséhez és integrálásához szükséges biztonsági és rendszerfelügyeleti szolgáltatások területén. Az új Novell kiemelt területei a Linux, a Biztonság, és a Rendszerfelügyelet – ahol a mobil eszközöktől az adatközpontokig kínálunk megoldásokat. Széles körű iparági támogatottságunknak köszönhetően megoldásaink kiválóan együttműködnek a vezető gyártók termékeivel.

Kiadványunkkal ahhoz szeretnénk segítséget nyújtani, hogy az informatikai rendszer, amely ma már a legtöbb szervezet alapvető üzletmenetét meghatározza, egy jól működő, megbízható és egységes infrastruktúraként működjön – az Ön vállalatánál is. A megbízható hálózati szolgáltatásokat ma a NetWare következő verziója, a linuxos Open Enterprise Server 2 kínálja. A NetWare frissítése Novell Open Enterprise Server 2-re egy világos és egyértelmű, automatizált művelet, ami észrevehetetlen a felhasználók számára. Ma már elképzelhetetlen a kommunikáció mobil készülékek nélkül, így a mobil végpontok védelme is egyre nagyobb szerephez jut. A hagyományos biztonsági intézkedéseket olyan új megoldásokkal kell kiegészíteni, amelyek közvetlenül az új fenyegetéseket veszik célba: a Novell ZENworks Endpoint Security Management a munkaállomásokra és laptopokra vonatkozó céges biztonsági irányelvek központi meghatározását, és ezek folyamatos kikényszerítését segíti. ZENworks rendszerfelügyeleti termékcsaládunk tíz éves fennállása óta számos új termékkel bővült, legutóbb az adatközpont-felügyelet egyik vezető szállítója, a PlateSpin felvásárlásával egészült ki a termékpaletta.

Kellemes és hasznos informálódást kívánok!

Szittyá Tamás,
üzgvezető igazgató

TARTALOM

4 Hírek

CIO

8 Az új Novell – Linux, biztonság, rendszerfelügyelet
Magyarországon is bemutatkozik az „új Novell”

TERMÉK

12 Tízből tízes

A ZENworks új kiadással ünnepli 10. születésnapját

17 Egységben az erő az adatközpontokban

Az adatközpontot lényegesen egyszerűbb és hatékonyabb egységes eszként kezelni

TECHNOLÓGIA

22 Biztonság már a mobil végpontokon is

Ma már elképzelhetetlen a kommunikáció mobil készülékek nélkül - de vajon biztonságosan használjuk őket?

25 Frissítés NetWare-ről?

A funkciókban gazdag Open Enterprise Server 2 előnyei a Windows Serverhez képest

Ingyenes terjesztésű kiadvány Novell Connection – A hálózati szakértők magazinja

Novell Kft. MOM Park, Sas torony, 1124 Budapest, Csörsz utca 45. Tel.: 36 1 489-4600; E-mail: info@novell.hu; www.novell.hu
Felelős kiadó: Szittyá Tamás – Felelős szerkesztő: Hargitai Zsolt – Stúdió munkálatok: Sásdi Gábor – Fordítási és egyéb munkák: Morpho Communications.

Connection a Világgal

> Az ország egyik legnagyobb jogosultságkezelő rendszerét építette ki a Novell a Magyar Telekom számára

Novell személy-azonosság- és jogosultságkezelési megoldásának hazai vezető szerepét erősíti, hogy a Magyar Telekom Csoport is a Novell Identity Manager megoldását választotta jogosultságkezelési folyamatainak konszolidálásához. A Novell tanácsadói csapata és a Novell Identity Manager teljesítette legjobban az elvárásokat. A Novell Magyarország vezető pozícióját tovább erősíti a hazai személyazonosság alapú biztonsági megoldások piacán, hogy 2008. májusában a HP és a Novell kizárólagos szövetséget jelentett be nemzetközi szinten, melynek keretében a HP Identity Center felhasználói egyszerűen térhetnek át a Novell személyazonosság-kezelési és biztonságfelügyeleti megoldásaira. A Novell Magyarország regionális konzultációs részlege a központi technológiai együttműködés tapasztalatait felhasználva felkészült a magyarországi átállások megvalósítására, illetve a résztvevő partnerek támogatására, és 50 %-os kedvezményt nyújt a konzultációs szolgáltatás árából. N

> A Novell 2008-as második pénzügyi negyedévében 7%-kal nőtt a termékértékesítésből származó árbevétel

A Novell bejelentette a 2008. április 30-án lezárult második pénzügyi negyedévének eredményeit. A vállalat árbevétele ebben a negyedévben elérte a nettó 236 millió amerikai dollárt, míg a 2007-es második pénzügyi negyedévben ez az összeg nettó 232 millió dollár volt. A működési eredmény a 2008-as második pénzügyi negyedévben 2 millió dollár volt, ezzel szemben 2007-ben ugyanebben az időszakban 12 millió dollár működési veszteséget könyvelhettek el. A folyamatos működésből származó eredmény a 2008-as második pénzügyi negyedévben 6 millió dollár, illetve részvényenként 0,02 dollár volt. A devizaárfolyamok kedvezően hatottak a árbevételre, ami 8 millió dolláros növekedést eredményezett. A Linux platformból származó árbevétel 31%-kal, a személyazonosság-kezelési és biztonság-felügyeleti megoldásokból származó termékbevétel 13%-kal, a rendszer- és erőforrás-felügyeleti megoldásokból származó árbevétel pedig 15%-kal nőtt az előző év azonos időszakához képest. N

> A Novell bejelentette a SUSE Linux Enterprise 10 Service Pack 2 elérhetőségét

A Novell bejelentette a SUSE Linux Enterprise 10 Service Pack 2-t (SP2), amely a virtualizáció, a felügyeleti eszközök, a hardvertámogatások és a rendszerek közötti együttműködés terén tartalmaz új fejlesztéseket. A SUSE Linux Enterprise Server 10 SP2 az egyetlen olyan Xen-alapú virtualizációs megoldás, amelyen a Microsoft teljes mértékben támogatja a Windows Server 2008 és a Windows Server 2003 vendégrendszereket, valamint ezek működés közbeni átvitelét a fizikai gépek között. A szervizcsomag a SUSE Linux Enterprise Desktop 10 és a SUSE Linux Enterprise Real Time 10 rendszerhez készült

fejlesztéseket is tartalmazza. A Novell emellett bemutatta a SUSE Linux Enterprise előfizetés-felügyeleti eszközét, amellyel az ügyfelek egyszerűbben kezelhetik a SUSE Linux Enterprise szoftverfrissítéseit. N

> Integrált biztonsági megoldások a Novelltól SAP vállalati rendszerekhez

A Novell bejelentette az iparág legátfogóbb integrált személyazonosság- és biztonsági eseménykezelési megoldásait, amelyek az SAP üzleti szoftveralkalmazásokra optimalizáltak. A Novell hat különböző biztonsági terméke integrált az SAP megoldásokra épülő környezetekkel, így az ügyfelek továbbra is a legtöbbet hozhatják ki befektetéseikből.

A vállalatok és intézmények átfogó felügyeleti igényeihez igazított Novell személyazonosság- és biztonsági eseménykezelési termékek kiegészítik az SAP irányítási, kockázati és megfelelőségi megoldásait (GRC), valamint a humánerőforrás- és vállalatirányítási (ERP) rendszereket. A Novell személyazonosság- és biztonsági eseménykezelési megoldásainak segítségével az SAP-ügyfelek hatékony, házi rend alapú felügyeleti funkciókat használhatnak, amelyek lehetővé teszik a felesleges adminisztrációs költségek csökkentését, automatizálják a bonyolult és hibákat eredményező manuális folyamatokat, leegyszerűsítik a jelszavak kezelését és pillanatok alatt alkalmazkodnak a változó alkalmazotti struktúrához. N

> A Novell a SUSE Appliance Programmal segíti a független szoftverszállítókat saját készülékeik fejlesztésében

A Novell bejelentette a SUSE Appliance Program elindítását, melylyel a független szoftverszállítók (ISV-k) olyan készülékeket fejleszhetnek, amelyeken a saját alkalmazásaik SUSE Linux Enterprise platformon futnak, és ezeket egyetlen integrált csomagban telepíthetik a végfelhasználóknál. A vállalat emellett a SUSE Linux Enterprise JeOS (Just enough Operating System) béta verzióját is bejelentette, amely a díjnyertes SUSE Linux Enterprise platform minimalizált változata. Ezt a megoldást a független szoftverszállítók platformként használhatják készülékeik fejlesztésekor és ennek köszönhetően egyszerűbbé válhat az alkalmazástelepítés és támogatás, jelentősen csökkenthetőek a fejlesztési költségek, és a végfelhasználók számára is könnyebbé válhat az alkalmazások telepítése. A SUSE Appliance Program kulcsfontosságú összetevője, a SUSE Linux Enterprise JeOS bétaverziója, amely virtuális lemezképként számos formátumban elérhető, például VMware VMDK, Xen, valamint nyers merevlemezképként. A Microsoft VHD formátumú SUSE Linux Enterprise JeOS megjelenése a Microsoft Hyper-V rendszerének kiadását követően még az idén várható. N

> Biztonságos online sportfogadás és szerencsejáték a Novell megoldásaival

A Novell bejelentette, hogy a bwin Csoport, az egyik vezető online sportfogadási és szórakoztató weboldal tulajdonosa a Novell megoldásait választotta megfelelősségi feladatainak hatékonyabb elvégzéséhez és informatikai infrastruktúrájának biztonságosabbá tételéhez. A bwin Csoport szolgáltatásait

több millióan használják fogadásra, pókerezésre, online szerencsejátékokra és más játékokra az interneten és egyéb digitális csatornákon keresztül. Így a több millió ügyfél, a több ezer belső felhasználó és a több száz alkalmazás, illetve adatbázis miatt a bwin-nek jelentős időt és energiát kellett fordítania a PCI-DSS szabvány szerinti megfelelőségi jelentések elkészítésére. A Novell biztonság- és információ-felügyeleti megoldása, a Novell Sentinel segítségével a bwin automatikusan felismeri a felhasználók adatait fenyegető veszélyeket, emellett megfelel a bankkártyákra vonatkozó szigorú iparági adatbiztonsági szabvány (Payment Card Industry Data Security Standard – PCI-DSS) követelményeinek ezzel csökkentve a megfelelőségi költségeket és erőforrásigényeket. **N**

> A „Szezám utcában” a Novell teszi hatékonyá az eszközkészlet felügyeletet és virtualizációt

A Novell bejelentette, hogy a Sesame Workshop – a „Szezám utca” című gyermeksorozat mögött álló non-profit oktatási célú szervezet – a Novell megoldásait választotta hardver- és szoftver-infrastruktúrája korszerűsítéséhez. A szervezet szoftverlicenceiről, -leltárairól és -használatáról teljes és pontos képet nyújtó Novell ZENworks Asset Management segítségével a Sesame Workshop hatékonyabban meg tud felelni az auditálási kéréseknek és megfelelően tudja kezelni lízing-szerződéseit. A SUSE Linux Enterprise Serverbe épített Xen virtualizáció segítségével pedig a szervezet 80 százalékkal csökkentette webszerverének helyigényét, 30 százalékkal pedig hardverköltségeit, mivel ezzel a megoldással a virtuális webkiszolgálókról több weboldalt is képes üzemeltetni. A nyílt forráskódú szoftverekben rejlő lehetőségek kihasználásával a szervezet jelentősen mérsékelte szoftverköltségeit, ami hozzájárult a teljes informatikai kiadás 18 százalékos csökkentéséhez. **N**

> A Novell és az Atos Origin globális partneri megállapodást kötöttek innovatív megfelelőségi és irányítási megoldások szállítására

A Novell és az Atos Origin – nemzetközi informatikai szolgáltatóvállalat – bejelentették új megfelelőségi és irányítási megoldások szállítását célzó partneri megállapodásukat. A Novell díjnyertes személyazonosság-kezelési és biztonságfelügyeleti megoldásai az Atos Origin tanácsadási, rendszerintegrációs és felügyelt üzemeltetési szolgáltatásaival olyan teljes körű megoldásokat kínálnak majd ügyfeleik számára, melyekkel még a legszigorúbb biztonsági, irányítási és megfelelőségi követelményeknek is megfelelnének. Ennek eredményeképpen az ügyfelek automatizálhatják a felhasználó erőforrás-kiosztást, hozzáférési-engedélyezési és biztonság-felügyeleti folyamataikat, mellyel költségeik mellett kockázataikat is csökkenthetik. A Premiere, Németország vezető kábeltelevízió szolgáltatója, és az INEM, a spanyol munkaügyi hivatal elsőként döntöttek a Novell és az Atos Origin közös ajánlata mellett. **N**

> A Novell ismertette a SUSE Linux Enterprise 11 várható fejlesztéseit

A Novell bejelentette következő generációs vállalati Linux platformja, a SUSE Linux Enterprise 11 fejlesztési terveit. A SUSE Linux Enterprise az egyetlen olyan Linux platform, amely a Microsoft, az SAP és a Capgemini által is elsődlegesen ajánlott és támogatott. A Novell a SUSE Linux Enterprise 11-gyel a

legjobb és legmagasabb szintű együttműködést biztosító kulcsfontosságú számítástechnikai platformot kínálja majd, amely a modern informatikai szervezetek központi elemévé válhat. Ez a platform a kulcsfontosságú vállalati folyamatok alapjaként a kiszolgálóvirtualizáció, a konszolidáció és a technológiai újítások mellett az ügyféloldali számítástechnika területén is áttörést jelent. Ennek köszönhetően az ügyfelek megtapasztalhatják a rugalmasság, a hatékonyság és a gyors reakció új szintjeit, függetlenül attól, hogy a SUSE Linux Enterprise rendszert közvetlenül a hardverre vagy egy virtuális gépre telepítik. A SUSE Linux Enterprise kulcsszerepet tölt majd be a vállalat céljának megvalósításában: segíti a világszerte működő szervezeteket a vegyes informatikai környezetek integrálásában, támogatva ezzel az emberek és a technológia együttműködését. A SUSE Linux Enterprise 11 a kulcsfontosságú adatközpont technológiák, a UNIX-átterési képességek, a virtualizáció, az együttműködés, a zöld informatika és az asztali Linux rendszerek területén kínál majd újításokat. **N**

> A Novell felvásárolja a PlateSpin-t, az adatközpont-felügyelet vezető szállítóját

A Novell bejelentette, hogy szerződést kötött a PlateSpin Ltd. felvásárlásáról, mellyel tovább növeli vezető szerepét a következő generációs adatközpontok területén. A 205 millió dolláros (napi árfolyam) tranzakció előreláthatólag hónapokon belül lezárul. A jövőben a Novell szállítja az egyetlen olyan megoldást, amellyel a fizikai és a virtuális környezetben egyaránt biztosíthatók az üzletmenet szempontjából fontos szolgáltatások. A PlateSpin átfogó megoldásokat kínál a fizikai vagy virtuális számítógépek heterogén munkaterhelésének – az adatok, alkalmazások és operációs rendszerek – felügyeletéhez. Ezek a megoldások javítják a kiszolgálókonszolidáció, az adatközpont-áttelepítés és a katasztrófa utáni helyreállítás sebességét és minőségét. A Novell és a PlateSpin megoldásai támogatják majd a vegyes forráskódú informatikai környezeteket, termékeikkel a munkaterhelések teljes életcikluskezelését és optimalizálását kínálják a fizikai és virtuális adatközpontban működő Linux, UNIX és Windows operációs rendszerekhez. A közös megoldások hozzásegítik az ügyfeleket a költségek csökkentéséhez, a szolgáltatási szint növeléséhez, valamint a változó üzleti követelmények teljesítéséhez. **N**

> A Novell új felügyeleti megoldása biztonságot nyújt a vállalati adatoknak mobil eszközökön is

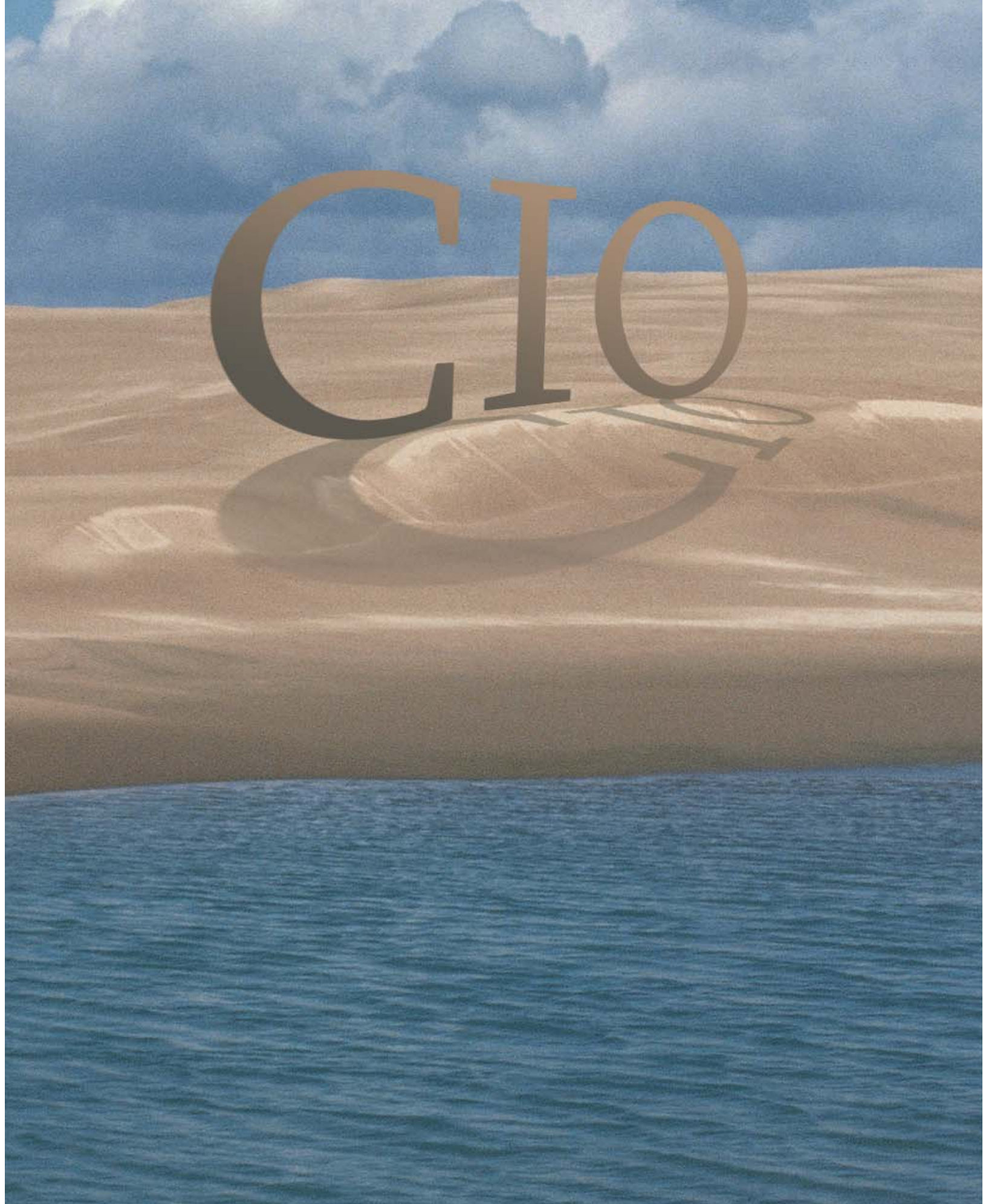
A Novell bejelentette a kibővített titkosítási funkciókkal rendelkező Novell ZENworks Endpoint Security Management végpontbiztonsági felügyeleti megoldásának elérhetőségét. A továbbfejlesztett házirendalapú biztonsági megoldás a személyes adatkezelés, az eltávolítható adattárolók és az engedélyezett eszközök magasabb szintű titkosítása mellett a beépített lemezek nagyobb fokú biztonságát is garantálja. A Novell ZENworks Endpoint Security Management megoldással a vállalati ügyfelek kifinomultabban szabályozhatják a végponti portokat és eszközöket, így még biztonságosabbá tehetik a vállalati adatokat. A Novell ZENworks Endpoint Security Management kibővített USB-felügyeleti eszközöket kínál a nem adattároló típusú perifériák, például az egerek és a nyomtatók kezeléséhez, így a rendszergazdák különböző feltételek, például a gyártó neve és az eszköz modellszáma alapján irányíthatják az eszközök hálózati hozzáférését. **N**

CIO

A természet adta lehetőségek kézzelfogható megoldásai

Az új Novell – Linux, biztonság, rendszerfelügyelet
Magyarországon is bemutatkozik az „új Novell”

CIO



Az új Novell – Linux, biztonság, rendszerfelügyelet

Magyarországon is bemutatkozik az „új Novell”

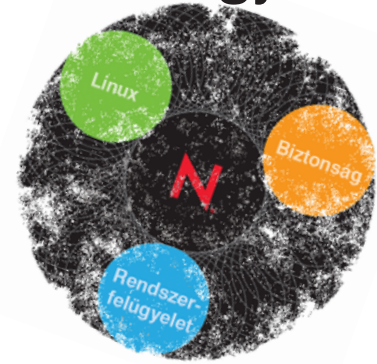
A

Novell Magyarország idén májusban a Brainshare magyarországi állomásán, éves technológiai konferenciáján ismertette az új Novell kínálatát a hazai szakmai közönséggel. A Novell hagyományosan a hálózati infrastruktúra szoftverek vezető szállítójaként alapozta meg elismertségét az iparágban. Az elmúlt évek azonban jelentős változásokat eredményeztek, hiszen a vállalat a kialakított stratégiai területeken saját kompetenciáját számos felvásárlással és piacvezető, innovatív technológiák integrálásával egészítette ki. Az együttműködést javító SiteScape, a virtualizációt és a munkaterhelés-felügyeletet megvalósító PlateSpin felvásárlásával, valamint az SAP, az Atos Origin és más piacvezető cégekkel kialakított partnerkapcsolatnak köszönhetően a Novell lendületesen fejlődik és mára a vállalati szoftvermegoldások egyik vezető szállítójává vált. Világszerte vezető szerepet tölt be a Linux-alapú és nyílt forráskódú vállalati operációs rendszerek, valamint a vegyes forráskódú, heterogén informatikai környezetek működtetéséhez és integrálásához szükséges biztonsági és rendszerfelügyeleti szolgáltatások területén. Az új Novell kiemelt területei a Linux, a Biztonság, a Rendszerfelügyelet – a mobil eszközöktől az asztali munkaállomásokon keresztül az adatközpontokig kínál átfogó megoldásokat Hol tart most és merre tart a Novell? A továbbiakban részletesebben bemutatjuk az új Novell kiemelt területeit: Linux, Biztonság, Rendszerfelügyelet, amelyekre a kategóriájában legjobb megoldásokat szállítja.

> Linux – aki kimarad, lemarad

Az új Novell első kiemelt területe a Linux. A Novell ma az operációs rendszerek piacán tör vezetői pozícióra, a Linux dinamikus térhódításának nyomán. A Novell által 2004-ben felvásárolt SUSE Linux a leggyorsabban növekvő vállalati Linux disztribúció a világon. Ma Magyarországon a Novell a legnagyobb vállalati Linux szállító. A magyarországi terméktámogatási központ, az NPSH pedig egyben a dél-kelet-európai régió központi termék-támogatási központja is. Aki ma nem kezdi el aktívan használni a linuxos technológiákat, komoly versenyhátrányba kerülhet, mert a Novell Linux megoldásai költséghatékonyak, emellett stabil megoldást nyújtanak a mobil munkaállomásoktól a mainframekig. A Novell célja Linux területen, hogy a Novell SUSE Linux alapértelmezett operációs rendszer legyen a szer- ver- és adatközpontokban.

A Novell SUSE Linux Enterprise rendszere jelenleg a legszélesebb körű iparági támogatással rendelkezik, a HP, az IBM, a



Microsoft, az SAP, az Oracle, az Intel és az AMD által. A SUSE Linux Enterprise a vállalati számítástechnika legjobb mérnöki hátterével széleskörű együttműködést biztosít a munkaállomásoktól egészen az adatközpontokig. Beépített virtualizációs technológiát kínál, és támogatja az adatközponti üzleti alkalmazásokat. Emellett a SUSE Linux Enterprise platformra építve további értéknovelt megoldásokat is kínál a vállalat, többek között a fájlárolási, nyomtatási és egyéb üzleti szolgáltatásokat nyújtó Novell Open Enterprise Server 2-t, amely a Novell hálózati szolgáltatásainak teljes 64 bites támogatását kínálja, valamint virtualizációt, megnövelt alkalmazás- és hardvertámogatást, és új tároláskezelési szolgáltatásokat is nyújt.

SUSE Linux alapú megoldások

- N- SUSE Linux Enterprise:** nyílt forráskódú vállalati Linux szerver és munkaállomás környezet.
- N- Open Enterprise Server:** SUSE Linux Enterprise alapú megoldás a Novell saját fejlesztésű komponenseivel.

2006 novemberében a Microsofttal kötött stratégiai együttműködési megállapodás nyomán világszerte számos nagyvállalat vezetett be SUSE Linuxot, többek között a PSA Citroen, a Renault, a Deutsche Bank, illetve az HSBC. Az egyezség alapján a Microsoft lett a Novell legnagyobb Linux-vezetője, de ennél fontosabb, hogy a két cég közös fejlesztői központot hozott létre, ahol többek között felügyeleti és címtár-megoldásaik kompatibilitásán, illetve az Office Open XML és OpenDocument Format átjárhatóságán dolgoznak. Emellett a két vállalat egyik kiemelt együttműködési területe a virtualizációs technológiák továbbfejlesztése. A Novell által kínált SUSE Linux Enterprise Serverbe beépített Xen alapú virtualizációs technológiával hatékonyabban szervezhető a vállalati informatikát érő csúcsterhelések és jelentősen lecsökkenthető a hardverköltések. A PlateSpin felvásárlása pedig tovább erősíti a Novell nyílt forráskódú virtualizációban betöltött vezető szerepét, mivel olyan eszközöket biztosít, amelyekkel az ügyfelek könnyedén helyezhetik át a fizikai munkaterheléseket a SUSE Linux Enterprise rendszeren futó Xen-alapú virtuális számítógépekre. A Microsoft és a Novell nemrégiben a kínai piacra is kiterjesztették együttműködésüket, amely a közös marketingtevékenységre és a képzésre irányul.

> Biztonság mindenképp felett

„Hatékony nagyvállalati biztonsági rendszer ma nem létezik hatékony személyazonosság-kezelés nélkül. A Novell a

Aki ma még nem kezdett el építeni a Linuxra, az lemarad

Az informatikai biztonság a hatékony személyazonosság-kezeléssel kezdődik

A Novell automatizált rendszerfelügyeletet biztosít a mobil munkaállomásoktól az adatközpontokig.

személyazonosság-kezelés egyik vezető vállalata.*” A személyazonosság alapú biztonsági megoldások használata mára elengedhetlenné vált az üzleti szférában. A Novell technológiája lehetővé teszi a személyazonosságok kezelését, illetve hatékony szabályozását mind az automatikus, mind az emberi beavatkozást igénylő folyamatok terén. A személyazonosság-felügyeletnek köszönhetően egyszerűbb javítani a szolgáltatásokon, könnyebb eltüntetni a biztonsági réseket és csökkenteni az informatika adminisztrációs költségeit. Éppen ezért a személyazonosság-kezelési megoldások piaca a Forrester előrejelzése szerint 2014-re várhatóan 12,3 milliárd dollárra nő.

A Novell automatizált biztonsági és megfelelőségfigyelési szolgáltatásokkal segíti a megfelelőségi követelmények betartását és a kockázatok csökkentését. Ezek a megoldások a teljes vállalatra kiterjedően automatizálják, ellenőrzik és betartatják az irányítási követelményeket, és lefedik mind a virtuális mind a fizikai eszközök körét. Közben tarthatók a felhasználók felügyeletével kapcsolatos költségek, megszüntethetők az összetett kézi folyamatok, és automatizmusokkal garantálható a biztonság, és az előírásoknak való megfelelés a vállalat teljes egészére – úgy, hogy közben a felhasználók azonnal elérik a munkájukhoz szükséges összes erőforrást.

Az IDC Magyarország, független piaci elemző cég felmérése szerint a Novell Identity Manager megoldása 33 százalékos piaci részesedéssel piacvezető** Magyarországon a személyazonosság alapú biztonsági megoldások területén. Ez a részesedés tovább növekedhet a Novell és a HP szövetségének köszönhetően, amelynek keretében a HP Identity Center felhasználói egyszerűen térhetnek át a Novell személyazonosság-kezelési és biztonságfelügyeleti megoldásaira.

Mindezen saját erőből, illetve saját fejlesztéssel megvalósított személyazonosság- és hozzáférés-kezelési megoldások mellett az utóbbi évek felvásárlásaival számos új termék került a Novell tulajdonába. Ide sorolható a Sentinel biztonsági információ- és eseménykezelő megoldás, vagy a Senforce felvásárlásából született ZENworks Endpoint Security végpontvédelmi szoftver. A díjnyertes Novell Sentinel automatizálja az informatikai szabályozás hatékonyságának figyelését, így a fenyegetések valós időben észlelhetők és oldhatók meg. A cég biztonsági portfóliója ezzel kibővült, és a legtöbb termék már hazai vállalati vagy intézményi referenciával is büszkélkedhet.

*Gartner - "Magic Quadrant for User Provisioning 2H07", IDC - White Paper: Identity and Security Management


** IDC Magyarország - Személyazonosság alapú biztonsági megoldások piaca, 2006.

Novell megoldások a kulcsfontosságú biztonsági célok eléréséhez

- N- Személyazonosság-kezelés: Novell Identity Manager
- N- Hozzáférés-felügyelet: Novell Acces Manager
- N- Biztonsági eseménykezelés és logelemzés: Novell Sentinel
- N- Egyponos bejelentkezés: SecureLogin
- N- Munkaállomás biztonsági megoldás: ZENworks Endpoint Security

> Rendszerfelügyelet

A Novell harmadik pillére a rendszerfelügyelet: a ZENworks termékcsalád a biztonsági termékekhez hasonlóan részben „saját erőből”, részben felvásárlások révén fejlődik. A cél, hogy a vállalatok átláthatóak és közben tarthassák informatikai vagyonukat, legyen szó mobiltelefonokról, kézi számítógépekről, noteszokról, PC-kről, vagy szerverekről, illetve hálózati berendezésekről. Ezen a területen nemrég a PlateSpin felvásárlásával erősített a Novell, és adatközpont-felügyeleti megoldásokkal bővült rendszerfelügyeleti termékportfóliója.

A Novell segítségével egységesítheti az informatikai rendszerek működését, mert a vállalat által kínált informatikai infrastruktúra igazodik az üzleti igényekhez, és a költségek szabályozása mellett alacsonyabb üzemeltetési és pénzügyi kockázatot biztosít. A Novell ZENworks rendszer olyan többplatformos rendszerfelügyeleti csomagot nyújt, amelynek segítségével automatizálhatja a hálózati eszközök, számítógépek, operációs rendszerek, alkalmazások és egyéb informatikai erőforrások felügyeletét. A PlateSpin megoldásaival kiegészülve a Novell olyan szabadságot és reakcióképeséget biztosít, amelyekkel átléphetők a fizikai és virtuális infrastruktúra határai és az informatikai rendszer egy egységként működtethető. A PlateSpin technológia egységesített munkaterhelés-felügyeleti keretrendszert biztosít, amely elosztja a terhelést a heterogén fizikai és virtuális infrastruktúrán belül. A Novell és a PlateSpin együttműködve biztosítja az átláthatóságot, a rugalmasságot és gyors a reakcióképeséget, hogy informatikai rendszere megfelelhessen a változó üzleti követelményeknek. 

A Novell teljes menedzsment portfóliója

- N- Munkaállomás-felügyelet: ZENworks Configuration Management
- N- Linux-felügyelet: ZENworks Linux Management
- N- Vagyongazdálkodás: ZENworks Asset Management
- N- Kéziszámítógép-felügyelet: ZENworks Handheld Management
- N- Patch menedzsment: ZENworks Patch Management
- N- Adatközpont felügyelet: PlateSpin termékcsalád

Termék

*„A képzelet az alkotás kezdete.
Elképezzük amire vágyunk, azt akarjuk amit elképezzük, s végül megalkotjuk amit akarunk.”
–George Bernard Shaw–*

Tízből tizes

A ZENworks új kiadással ünnepli 10. születésnapját

Egységben az erő az adatközpontban

Az adatközpontot lényegesen egyszerűbb és hatékonyabb egységes eszkézként kezelni



Tízből tizes

A ZENworks új kiadással ünnepli 10. születésnapját



A Novell csapata 1998-ban egy új, innovatív termékkel jelentkezett, amelynek a Z.E.N.works nevet adták. Emlékszik még, hogy miért vannak a betűk után a pontok? Azért, mert ez a Zero Effort Networking rövidítése. A termék – nevéhez híven – több órányi munkát takarít meg a vállalatoknak és intézményeknek az informatikai környezet felügyelete során, a munkaállomásoktól kezdve az adatközpontokig. 2008-ban már a ZENworks megjelenésének tizedik évfordulóját ünnepelhetjük!

Tíz év alatt sok minden megváltozott. A ZENworks stratégiai termékcsaláddá vált a Novell termékínalatában. A termékcsaládot egy új megoldással: a ZENworks 10 Configuration Managementtel bővítettük. A termék háromféle kiadásban kapható, így az Ön igényeinek leginkább megfelelő funkciókat kínálja (lásd 1. ábra cikk végén).

> Új terminológia

A ZENworks 10 Configuration Managementben számos olyan fogalom módosul, amit a tradicionális ZENworks-felhasználók a különféle objektumokra és beállításokra történő hivatkozásnál használtak. Új fogalmakat is bevezettek. Az alábbiakban néhány új fogalmat ismertetünk:

Zóna (Zone): A zónák a felügyelet legnagyobb és egyben legkisebb egységei a ZENworks 10 Configuration Managementben. A zóna egy vagy több elsődleges szerverből, felügyelt eszközökből, tartalmelosztási pontból és az összes olyan felügyeleti objektumból áll, amelyek hozzárendelhetők ezekhez az eszközökhöz, valamint azon felhasználókból, akiknek hozzáférését a zóna hivatott biztosítani.

Elsődleges szerver (Primary Server): Az elsődleges szerver az a gép, amelyen a Tomcat webservert, a webszolgáltatások és a tartalomlerakat – amely a tartalomnak a zónába tartozó eszközökre történő szétosztásához szükséges – található. Az elsődleges szerver lehet Windows 2003, SUSE Linux Enterprise 10 vagy Open Enterprise Server 2, mindhárom esetben akár a 32, akár a 64 bites változat.

Tartalmelosztási pont (Content Distribution Point): A tartalmelosztási pont egy felügyelt Windows munkaállomás vagy szerver, amelyet úgy állítottak be, hogy forrásként működjön, ahonnan a többi felügyelt eszköz

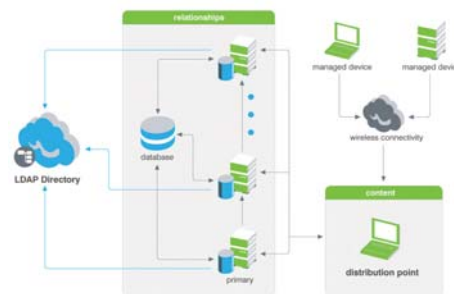
lekerheti a termékcsomag (bundle) vagy irányelv tartalmat.

ZENworks Control Center: A ZENworks Control Center a ZENworks 10 Configuration Management fő adminisztrációs eszköze. Egy webes konzol, amely Windows munkaállomásokon futó Microsoft Internet Explorer 6/7-ből vagy Mozilla Firefoxból is elérhető.

Felhasználói forrás (User Source): A felhasználói forrás egy mutató, amely egy olyan külső Active Directory Services vagy eDirectory szervert jelöl, ahonnan az elsődleges szervernek ki kell olvasnia a felhasználói, csoport- és konténeradatokat. A felhasználói forrás beállításával a forráson belül engedélyezhetők a ZENworks 10 Configuration Management irányelvek és a termékcsomagok felhasználóhoz történő hozzárendelése.

Szolgáltatásorientált architektúra

A ZENworks 10 Configuration Management a ZENworks szolgáltatásorientált architektúrát (Service Oriented Architecture – SOA) használja. Ez az architektúra egy több-rétegű modell, amelynek segítségével a ZENworks termékek még rugalmasabbá, stabilabbá és méretezhetőbbé tehetők (lásd 2. ábra).



2. ÁBRA: A komplex ZENworks SOA tartalmazza a menedzselte eszközöket, a jogosultságkezelő és a tartalomelosztási szinteket

A ZENworks SOA négy rétegből áll:

- A webszolgáltatási réteg tartalmazza a Tomcat servlet-alkalmazást és a ZENworks funkcióinak megvalósításáért felelős servleteket (szerver-kisalkalmazásokat).

Mindössze harminc percbe telik a ZENworks Configuration Management telepítése és elindítása. A ZENworks 10 Configuration Management tervezésénél az volt az egyik cél, hogy a termék a telepítés kezdetét követően fél órán belül használható legyen.

Minden servlet egy adott funkciót biztosít és a SOA más szintjein interaktívan együttműködik a többivel.

- Az adatmodell-réteg egy sor API-ból áll. Ezek lehetőséget biztosítanak arra, hogy a webszolgáltatások együttműködjenek a konfigurációs adatokkal anélkül, hogy megértenék az adattár alapvető jellemzőit. Így a ZENworks különféle adatbázisplatformokat használ anélkül, hogy az egyes szolgáltatásoknak ismerniük kellene az adatbázist, amellyel kommunikálnak.
- A ZENworks SOA tárolási rétege nagy mennyiségű, logikailag nem az adattárolóban elhelyezett adat tárolására használható. A ZENworks 10 Configuration Managementben a tárolási réteg tartalomlerakatként valósul meg – ez egy fájlrendszeri hely az egyes elsődleges szervereken. Ez a lerakat ad otthont az összes fájlnak, melyek alkalmazások, irányelvek, javítások és rendszerképek szétosztásához szükségesek.
- Opcionális az azonosítási réteg. Lehetővé teszi, hogy a ZENworks szolgáltatások interaktív módon együttműködjenek egy személyazonosság-tárolóval. A jelenlegi ZENworks SOA rendszerben az azonosítási réteg működik Active Directory Services és Novell eDirectory rendszerrel is. Az azonosítási réteg kihasználja a Novell Common Authentication Services Adapter (CASA) szolgáltatásának előnyeit.

Az architektúra további fontos eleme a ZENworks Adaptive Agent. A ZENworks Adaptive Agent és a ZENworks 10 Configuration Management Primary Server közötti kommunikáció általában szabványos webes munkamenetként valósul meg. A ZENworks előző változataitól eltérően a ZENworks Adaptive Agent nem tart fent egy munkamenetet az elsődleges szerverrel, hanem HTTPS-kérést intéz hozzá, megkapja a szükséges információkat, majd lecsatlakozik. Ezzel az elsődleges szerver több klienst tud kiszolgálni.

Ez az új architektúra számos előnyt nyújt: többé nem a ZENworks-ügynök végzi el a munka nagy részét. A szerveren futó webszolgáltatások kezelik az üzleti logikát, majd átadják az eredményeket az ügynöknek. Ez általában kisebb hálózati forgalmat és jobb méretezhetőséget eredményez. Az új architektúrával a későbbi szolgáltatások és funkciók hozzáadása is egyszerűbb.

> Legyen az idő pénz!

Mindössze harminc percbe telik a ZENworks Configuration Management telepítése és elindítása. A ZENworks 10 Configuration Management tervezésénél az volt az egyik cél, hogy a termék a telepítés megkezdését követően fél órán belül használható legyen. Ez azt jelenti, hogy Ön fél órán belül telepítheti az első elsődleges szervert, beállíthatja ezt egy vagy több felhasználói forrás elérésére, és telepítheti az ügynököt legalább egy eszközre a hálózatban. Cél volt a tervezésnél az is, hogy a

feladat befejezése után a ZENworks Adaptive Agentet egyszerűen rá lehessen helyezni a környezet bármelyik felügyelni kívánt eszközére.

A telepítés varázsló elindulása után a telepítőeszköz a következő feladatokat végzi el:

1. Telepíti a Tomcat szoftvert, ami a többi szolgáltatás telepítéséhez kell.
2. Telepíti a Tomcat által működtetett webes szolgáltatásokat, melyek ezután a szolgáltatási vezérlőpanelben (Services Control Panel) beállításra kerülnek ZENworks Server szolgáltatásként.
3. Telepíti és beállítja a ZENworks Loader szolgáltatást. Ez biztosítja a leltár, a csomagkezelés és a szerver alapú aszinkron műveletek elvégzéséhez szükséges leg fontosabb szolgáltatásokat, például az eszközök frissítését és más gyors elvégzendő feladatokat.
4. Telepíti a rendszerindítás előtti szolgáltatásösszetevőket (Preboot Service Components). Ezekre a PXE munkaállomások és a rendszerkép-kezelés támogatásához van szükség. Az összes szolgáltatás automatikusan elindul, kivéve a Proxy DHCP Servert.
5. Miután az elsődleges szerver szoftverét telepítették és elindult, a ZENworks Adaptive Agentet is telepíti, ha a telepítés Windows szerverre történt.
6. Végül létrejönnek a szerver számára szükséges fájlok és a ZENworks beállítási oldal. Ide manuálisan behúzhatók a telepítőfájlok, az átállási eszközök és a saját ZENworks környezet többi fontos fájlja.
7. Ha a Business Objects Enterprise telepítést választja, akkor települnek a ZENworks Configuration Management jelentéskészítő összetevői is.

A telepítés befejezése után a szerveroperációs rendszer szabványos eszközeivel ellenőrizheti a telepített ZENworks szolgáltatások állapotát. Egy böngészőbe írja be a `https://<szerver>/zenworks` címet. Ezzel ellenőrizhető, hogy a Tomcat webszerver működik-e és, hogy a ZENworks Control Center servlet sikeresen betöltődött-e.

> Csomagkészítés és átcsomagolás

Az alkalmazások terjesztésekor az alkalmazás csomagolása kritikus fontosságú lépés. Mire érdemes odafigyelni az alkalmazások csomagolása és átcsomagolása során? A követendő eljárások az alábbiak:

- Az átcsomagolást olyan géptípuson végezze, amelyre majd telepíteni fog. Az átcsomagolás során a Repackager eszközt javasolt ugyanolyan operációs rendszeren futtatni, mint amelyre az ügynököt telepíteni szeretné. Ez biztosítja, hogy ha az örökölt telepítő operációs rendszer specifikus funkciókat is tartalmaz, akkor azok szerepelnek majd a Microsoft telepítőcsomagban (MSI-ben).

Miért tölt órákat a virtuális gépek felügyeletével, mikor a Novell ZENworks Virtual Machine Management ezt elintézi Ön helyett?

- Használja a Global Exclusions Editort. Ha rendszeresen kizárja ugyanazokat a registry kulcsokat, fájlokat, vagy .ini információkat az MSI-ből, akkor vegye fel ezeket a Global Exclusions Editor-ba, így a Repackager automatikusan kihagyja őket.
- Csak akkor használja a Tuner alkalmazást, ha nincs gyártóspecifikus eszköz. Ezt azért ajánljuk, mert a gyártók sokkal jobban ismerik az MSI-t, mint a Macrovisiont, és sokkal több konfigurációs beállítást adhatnak meg.

> Irányelvek végrehajtása – könnyedén

A ZENworks 10 Configuration Managementben az „irányelvek” kifejezés több olyan konfigurációs beállítást és szabályt jelent, amelyeket egy felügyelt eszközön kell alkalmazni. Az irányelveket általában arra használják, hogy konfigurálják egy eszközön telepített szoftver (például Windows operációs rendszer, Microsoft Office termékcsomag vagy ZENworks Adaptive Agent) bizonyos részeinek működését.

A ZENworks 10 Configuration Management lehetőséget ad arra, hogy irányelveket rendeljünk felhasználókhoz (Users), munkaállomásokhoz (Workstations), csoportokhoz (Groups), dinamikus csoportokhoz (Dynamic Groups) és mappákhoz (Folders). Ezzel az irányelv-hozzárendelés rendkívül rugalmasá tehető.

> Átállás a személyiség-megőrzésével (Personality Migration)

Mit is jelent a személyiség? Ez a kifejezés az összes felhasználóspecifikus operációs rendszeri és alkalmazási beállításra, valamint adatra utal. Egy adott gép személyiségét ezek a beállítások, valamint a gépen található összes felhasználó adatai alkotják. A gépek személyiségét alkotó beállítások lehetnek például az adott felhasználó által használt háttérkép-beállítás és a tényleges háttérkép-fájl, a személyre szabott megjelenítési beállítások, az Internet Explorer és Mozilla Firefox beállítások, a biztonsági és egyéb konfigurációs beállítások. Ezeknek a beállításoknak és adatfájloknak az összessége és további egyéb elemek együttesen alkotják egy gép személyiségét. Emellett a gépen minden felhasználónak megvan a maga személyisége, ami a hozzá tartozó adatokból és beállításokból áll össze. Ha Ön ismeri a Windows profil fogalmát, akkor gondoljon úgy a személyiségre, mint a profilnál nagyobb halmazra, amelynek a profil a részhalmaza.

> Az eszközök nyomon követése

Ha nem tudja milyen eszközökkel rendelkezik, hogyan tudná felügyelni azokat? A ZENworks 10 Configuration Managementtel összegyűjthetőek az alábbi leltárinformációk:

- Hardverleltár: A ZENworks 10 Configuration Management többféle módszert használ a hardverinformációk Windows eszközökről történő begyűjtésére, melyek a ZENworks Adaptive Agentet és a Windows Inventory Only Agentet

használnak. Emellett azokról a Windows eszközökről is gyűjt hardverinformációkat, amelyeken a hordozható begyűjtő (Portable Collector) végrehajtásra kerül, vagy az OSX-et és Inventory Only ügynököt futtató Macintosh gépekről, vagy azokról a NetWare szerverekről, amelyeken az Inventory Only ügynök van telepítve. Az információ megszerzését szolgáló módszerek minden platformon mások lehetnek.

- Szoftverleltár: A ZENworks 10 Configuration Management ezekről a platformokról a szoftverinformációkat is bekéri. A Windows ügynökök és a hordozható begyűjtő a szoftver-tudásbázist használja a telepített szoftver azonosítására, valamint lekéri a gépről a végrehajtható állományok és más opcionális fájlok listáját is. A NetWare platformon a NetWare Products adatbázis tartalmának kigyűjtésével történik a szoftverleltár. Mac OS X-en a szoftverleltár a System Profiler alkalmazást használja.
- Termékcsomag-leltár: A ZENworks 10 Configuration Management a termékcsomag-leltári információkat is lekéri. Ez a ZENworks Adaptive ügynök lekérdezésével történik, innen határozható meg az eszközön telepített termékcsomagok neve és verziószáma. Ezzel egyszerűen nyomon követhetőek azok az eszközök is, melyekre a ZENworks 10 Configuration Management használatával termékcsomag került.

Az eszközeleltár szolgáltatásai kibővíthetők a ZENworks Configuration Management Enterprise Edition-ben megtalálható Asset Management Services használatával.

Hét termék hét nap alatt!

A ZENworks termékcsalád hét új tagja jelenet meg tavaly hét nap alatt:

- | | |
|---|--|
| 1. ZENworks Configuration Management Standard Edition | 5. ZENworks USB/Wireless Security Management 3.5 |
| 2. ZENworks Configuration Management Advanced Edition | 6. ZENworks Orchestrator 1.1 |
| 3. ZENworks Configuration Management Enterprise Edition | 7. ZENworks Virtual Machine Management 1.1 |
| 4. ZENworks Endpoint Security Management 3.5 | |

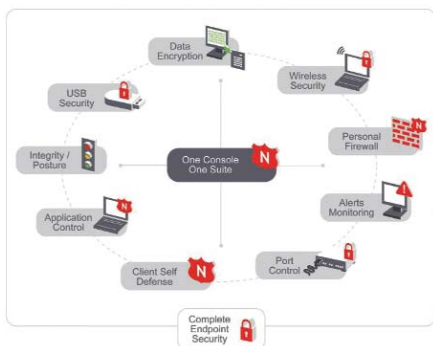
A ZENworks 10 Configuration Management integrált része a Business Objects Enterprise XI R2 változata. Ez az iparágvezető üzleti intelligencia-platform az adatbázisban található legtöbb információ esetében teljes rugalmasságot biztosít a jelentések végrehajtásához. A jelentéskészítés leegyszerűsítéséhez a ZENworks 10 Configuration Management egy előre beállított Business Objects Enterprise univerzumot tartalmaz (ez a táblák halmazát és az ezekhez tartozó meghatározó információk összességét jelenti), amely lehetőséget ad a jelentéskészítéshez szükséges legfontosabb mezők azonosítására, majd ezek használatával a jelentések összeállítására.

> A végpontok biztonságossá tétele

A Novell bejelentette a Senforce felvásárlását és két új termék – a ZENworks Endpoint Security Management és a ZENworks USB/Wireless Security – megjelenését. A két új

Ha nem tudja milyen eszközökkel rendelkezik, hogyan tudná felügyelni azokat? A ZENworks Configuration Managementtel könnyedén összegyűjthetők a leltárinformációk.

megoldás biztosítja az asztali és noteszgépek védelmét a vezeték nélküli és egyéb támadások, valamint a rosszindulatúan használt USB-eszközök ellen. A ZENworks Endpoint Security Management szolgáltatásait a 3. ábra mutatja be.



3. ÁBRA: A központi irányítás megtartásával, a Novell ZENworks Endpoint Security Management biztonságossá teszi a hálózati végpontok használatát

A végpont megfelelő védelméhez többek között szükség van a központosított felügyelet lehetőségére és egy konzolra. Emellett a funkciókat egyetlen csomagban kell tartalmaznia (egyetlen ár, egyetlen ügynökprogram). A hatékony működéshez a felhasználói funkcionalitás szűkítése nélkül kell célba vennie a fenyegetést és észlelni a sérülékeny pontokat. Ön minden bizonnyal azt szeretné, hogy a felhasználók a rendszerük konfigurálása, vagy javítgatása helyett a munkájukra koncentráljanak.

Kritikus fontosságú tényező az is, hogy ne a végfelhasználók döntsenek (ne legyenek például felugró ablakok és ennek következtében hibás döntések), hanem a biztonsági rendszergazdák hozzák meg azokat, illetve, hogy a rendszert ne lehessen megkerülni. Fontos továbbá a meglévő címtárszolgáltatásokkal és infrastruktúrával való integráció is.

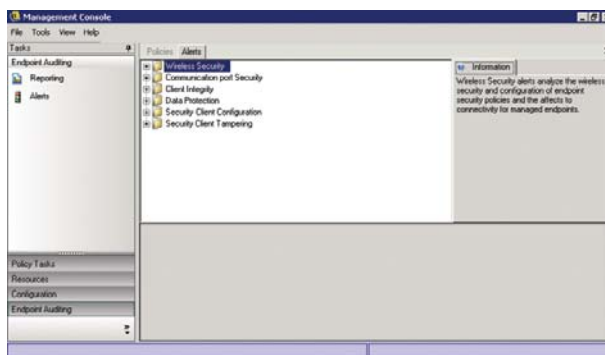
A Novell ZENworks Endpoint Security Management Alerts Monitoring biztosítja, hogy a cég biztonsági irányelveit veszélyeztető összes kísérletről jelentés kerüljön a felügyeleti konzolba. Ezáltal a rendszergazdák azonnal tudomást szerezhetnek a problémákról és megtehetik a megfelelő intézkedéseket.

A Riasztások (Alerts) kezelőfelület teljes egészében konfigurálható, így tökéletesen kézben tartható, hogy mikor és milyen gyakran érkezzenek aktivált riasztások (lásd 4. ábra).

A ZENworks Endpoint Security Management nem csak megfelel a hatékony biztonság összes követelményének, de jelentős előnyöket is kínál az alábbi tulajdonságok révén:

- Nagyobb reakciósebességet és hatékonyságot tesz lehetővé az ezekhez tartozó kockázatokat kezelésével.
- Védelmet biztosít a végponton tárolt és az eszköz által elért adatoknak.

- Védi az informatikai rendszert a felhasználói üzemidő - és így a hatékonyság - növelése érdekében.
- Csökkenti a költségeket azáltal, hogy egyetlen konzolt használ a beállításhoz, a felügyelethez, a jelentéskészítéshez, valamint a riasztásokhoz.
- Csökkenti a költségeket azzal, hogy egyetlen ügynökprogramot használ a biztonság kikényszerítéséhez.
- Célzott kikényszerítést biztosít bizonyos megadott problémák kezeléséhez, miközben maximalizálja a felhasználók hatékonyságát.
- Rákényszeríti a szakértők által meghatározott biztonsági döntések betartására a teljes szervezetet.

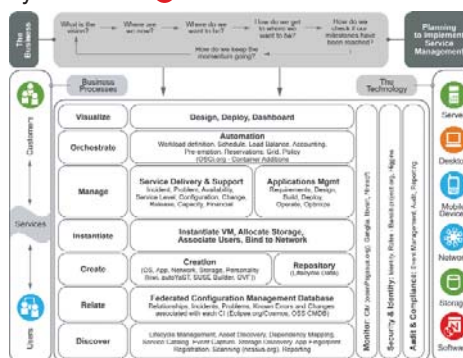


4. ÁBRA: A Riasztások (Alerts) kezelőfelület teljes egészében konfigurálható, így kézben tartható hogy mikor és milyen gyakran érkezzenek aktivált riasztások

> A vállalati kockázat enyhítése és az informatikai költségek csökkentése

Az új ZENworks termékek és a teljes ZENworks termékcsalád lehetőséget nyújt a sokféle eszközt, operációs rendszert, szoftvert és más informatikai erőforrást tartalmazó megosztott környezetek bonyolultságának, sérülékenységének és költségvetésének csökkentésére.

A Novell a munkaállomásoktól kezdve az adatközpontokig továbbra is biztosítja a hatékonyabb felügyelethez szükséges eszközöket (lásd 5. ábrát). Csatlakozzon hozzánk: ünnepeljünk együtt a ZENworks izgalmas évtizedét és találjuk ki együtt, hogyan hasznosíthatná Ön is a ZENworks előnyeit saját környezetében. **N**



5. ÁBRA: A Novell a munkaállomásoktól kezdve az adatközpontokig biztosítja a hatékonyabb felügyelethez szükséges eszközöket

A Novell ZENworks Endpoint Security Management Alerts Monitoring biztosítja hogy a cég biztonsági irányelveit veszélyeztető összes kísérletről jelentés kerüljön a felügyeleti konzolba – így a rendszergazdák azonnal tudomást szerezhetnek a problémákról és megtehetik a megfelelő intézkedéseket.

ZENworks Configuration Management A szolgáltatások áttekintése	Standard	Advanced	Enterprise
Felügyelt rendszerek	✓	✓	✓
Windows Vista	✓	✓	✓
Windows XP Professional	✓	✓	✓
Windows XP Tablet Edition	✓	✓	✓
Windows 2000 Professional	✓	✓	✓
Windows Server 2003	✓	✓	✓
Windows 2000 Server	✓	✓	✓
Macintosh OSX ***	✓	✓	✓
Windows NT4 ***	✓	✓	✓
Windows 98 ***	✓	✓	✓
Windows 95 ***	✓	✓	✓
NetWare 6.5 ***	✓	✓	✓
Alkalmazásfelügyelet	✓	✓	✓
Alkalmazások öngyógyítása	✓	✓	✓
Távoli felügyelet	✓	✓	✓
IT-eszközfelderítés és -osztályozás	✓	✓	✓
BusinessObjects jelentéskészítés	✓	✓	✓
Integrált javításkezelés*		✓	✓
Cserélhető média-eszközök szabályozása		✓	✓
USB-portok szabályozása		✓	✓
LAN-, modem-, Bluetooth, infra- és Firewire portok szabályozása		✓	✓
Soros és párhuzamos portok szabályozása		✓	✓
Wi-Fi hálózati elérés szabályozása		✓	✓
Az engedélyezett hozzáférési pontok listáinak felügyelete			✓
Adattitkosítás			✓
Személyi tűzfal			✓
Biztonsági riasztások figyelése			✓
Kliensek önvédelme			✓
Az engedélyezett alkalmazások felügyelete			✓
Alkalmazásblokkolás			✓
Integrált leltárkezelés			✓
Viszonteladói csatolók a vásárlási rekordok integrálásához			✓
Szoftvereszköz-licencek követése			✓
Szoftverhasználat követése			✓
Eszközszerződés-kezelés			✓
Kézi eszközök alkalmazásainak kezelése			✓
Kézi eszközök biztonsági felügyelete			✓
Kézi eszközök jelszósinkronizációja a hálózati biztonsági szolgáltatással			✓
Kézi eszközök távfelügyelete			✓
Linux-rendszerek kezelése			✓
Linux-eszközjavítások			✓
Linux-eszközök távoli felügyelete			✓

1. ÁBRA:

Egységben az erő az adatközpontokban

Az adatközpontot lényegesen egyszerűbb és hatékonyabb egységes egészként kezelni



Az üzleti folyamatok egyre inkább felgyorsulnak. Ahhoz, hogy a szervezetek lépést tudjanak tartani ezzel az ütemmel, olyan IT-infrastruktúrára van szükségük, amely azonnal reagál a folyamatosan változó üzleti feltételekre. Korábban az üzleti felhasználó új szolgáltatás iránti igénye esetén egyetlen alkalmazással vagy céllal rendelkező új fizikai szervert alakítottak ki. Ez a gyakorlat azonban drága, merev és nem igazán hatékony. Időközben megjelent a virtualizáció, amely új teljesítményszintet és hatékony eszközt biztosít az informatikai igazgató számára, lényeges viszont kiemelni, hogy önmagában nem csodafegyver.

A virtuális infrastruktúráknak együtt kell működniük az új és a már meglévő fizikai infrastruktúrákkal. Ez új felügyeleti kihívásokat támaszt a biztonság, az ellátás és az IT-költségek terén.

Az adatközpont rugalmasságához az adatközpont holisztikus felügyeleténél többre van szükség. Az üzlet igényeinek kielégítéséhez az asztali környezet és a szerver üzemeltetésében, a vezérlés módosításában, és a hozzáférés-felügyeletben is nagyobb gyorsaság kell. Eltérő megoldások szükségesek a módosítási projektek megtervezéséhez és végrehajtásához attól függően, hogy szerverkonsolidációról és virtualizációról, hardverátállításról vagy akár teljes adatközpont-áthelyezési kezdeményezésről van szó. A szervezetek költségcsökkentés és teljesítményjavítás céljából alkalmazzák ezeket a kezdeményezéseket. Sajnálatos módon ezek többsége kritikus késleltetést és szükségtelen kockázatot von maga után a nem megfelelő tervezés, vagy a működésüket segítő, megoldásra koncentráló termékek hiánya miatt.

> Az ideális megoldás-keretrendszer

A virtualizáció a szoftver és a hardver közötti kötés feloldásával arra ösztönzi a szervezeteket, hogy az adatközpontokra ne statikus szerverek gyűjteményeként tekintsenek, hanem hordozható terhelési egységek halmazaként. A legalapvetőbb szinten a terhelés a fizikai vagy virtuális hoszton lévő adatokat, alkalmazásokat és operációs rendszereket foglalja magában.

Olyan következő generációs felügyeleti megoldásra van szükség, amely megfelel a következő feltételeknek:

- A fizikai és virtuális környezeteket egyaránt jól kezeli.
- Segítséget nyújt az adatközpont felügyelői és tervezői számára, hogy gyártói kötöttségek nélkül a legjobb környezetet választhassák függetlenül attól, hogy az virtuális vagy fizikai.
- Olyan egyesített megoldás, amely kiértékeli a terheléseket, megmondja, melyik környezet a legjobb, majd biztosítja, áthelyezi, védi és optimalizálja ezt a környezetet annak élettartama során.

> A PlateSpin bemutatása

A torontói PlateSpinnek világszerte megközelítőleg 5000 ügyfele – a Fortune 500 közel felét is beleértve – van. Termékportfóliójában a többplatformos funkcionalitásra, valamint az együttműködésre koncentrál. Megoldásai segítségével a vállalatok elkülöníthetik a szerverterheléseket és az ezek alapjául szolgáló hardvert. Lehetővé teszik a terhelési egységek profiljának elkészítését, telepítését, áthelyezését, másolását, védelmét valamint replikálását az adatközpont tetszőleges helyén, a fizikai és virtuális határokon túl. A PlateSpin több mint 700 ezer sikeres szerverterhelés-átállítást hajtott végre – többet, mint a virtualizációs piac bármely más résztvevője.

A PlateSpin technológiája az IT-szakértők számára biztosítja az adatközpont terhelés alapú nézetét, ezáltal új lehetőségeket kínál a szervezetek számára a hatékony működés eléréséhez és a költségcsökkentéshez.

> Áthelyezés, Védelem, Kiszolgálás

A PlateSpin egy integrált termékcsaládot biztosít, amely automatizálja az adatközponti szolgáltatások kiértékelését és átállítását, ezáltal az ügyfelek csökkenthetik a költségeket, az energiafelhasználást és az adatközpont padlóján/rackjében elfoglalt területet. A PlateSpin egyesített katasztrófa-helyreállítási megoldása megfizethető terhelésvédelmet kínál, amely a virtualizációs technológiát is kihasználja az adatközpont fizikai és virtuális terheléseinek védelméhez, így nagyobb biztonságot és jobb üzletmenet-folytonosságot kínál. A PlateSpin-technológiák segítségével az ügyfelek platform függetlenül egyetlen megközelítést használhatnak a virtuális és fizikai terhelések képfájljainak elkészítéséhez és beállításához, így nincs szükség manuális telepítésre, és az új szerverterhelések kiszolgálásához lényegesen kevesebb idő szükséges.

A virtuális infrastruktúráknak együtt kell működniük az új és a már meglévő fizikai rendszerekkel is.

Ez új felügyeleti kihívásokat támaszt
a biztonság, az ellátás és az IT költségek terén.

> Folyamatos optimalizálás és felügyelet

A Novell és a PlateSpin együtt optimalizálják a fizikai és virtuális infrastruktúra közötti egyensúlyt. Automatizálják a megfigyelést, illetve a szerver rendelkezésre állása és a terhelési igények alapján infrastruktúra-beállításokat végeznek. Azáltal, hogy a kiegyenlítési folyamat automatikussá, átláthatóbbá vált és kiértékelésre kerül, hogy a terhelések hogyan használják a fizikai és virtuális erőforrásokat a különböző időpontokban, az ügyfelek hatékonyabban használhatják ki szervereik teljesítményét.

> PlateSpin és a Novell: Egyesített adatközponti megoldáscsomag

A PlateSpin termékek leegyszerűsítik az adatközponti problémák megoldását azáltal, hogy a szervezetek egységesen kezelhetik az általános terhelési életciklussal kapcsolatos problémákat. Azáltal, hogy a terhelések egyszerűen „áthúzhatók” a fizikai vagy virtuális hosztra – arra, ahol a leghatékonyabban futtathatók –, javítható a szerverkonszolidáció, a bérlethardver-átállítás, az adatközponti problémák megoldását azáltal, hogy a szervezetek egységesen kezelhetik az általános terhelési életciklussal kapcsolatos problémákat.

A Novell és a PlateSpin a fizikai és virtuális adatközpontokban is teljes terhelési életciklus felügyeletet és optimalizálást biztosítanak Windows, UNIX és Linux operációs rendszerekhez. A Novell és a PlateSpin egyedülálló termékportfóliót kínál a terhelések kezeléséhez az életciklus során a kiszolgálástól és védelemtől kezdve az áthelyezésig és optimalizálásig, legyen szó akár egy hatékony virtualizációs platformmal rendelkező teljes megoldáscsaládról, vagy akár a fizikai és virtuális infrastruktúra meglévő befektetéseit kihasználó, kategóriájában a legjobb heterogén felügyeleti megoldásról.

A kombinált Novell-PlateSpin megoldások komoly értéket képviselnek azáltal, hogy csökkentik a költséget, javítják a szolgáltatásszinteket és gyorsan reagálnak a változó üzleti követelményekre. A Novell és PlateSpin technológiákat – mérettől függetlenül – minden vállalat használhatja a fizikai és virtuális környezetek együttműködésének biztosításához.

A megoldás bevezetése az alábbi előnyöket biztosítja:

- Csökkenthető a költségek a szerverterhelések létesítéséhez, védelméhez, áthelyezéséhez és optimalizálásához szükséges idő lerövidítésével.
- Biztosítható a virtuális és fizikai terhelések dinamikus és automatikus kiszolgálásának rugalmassága és agilitása.
- Gyorsabban és rugalmasabban lehet reagálni az új IT erőforrások üzleti követelményeire.
- Javítható a szerver kihasználtsága azáltal, hogy több alkalmazás lehet egyszerre egy fizikai szerveren.
- Csökkenthető az energia- és hűtési igények a virtualizáció és a konszolidáció kihasználásával.

> PlateSpin PowerConvert 7.0: A Novell és a PlateSpin első közös fejlesztése

A PlateSpin és a Novell 2008. júliusában bejelentették az új biztonsági mentési és visszaállítási funkciókkal kibővített PlateSpin PowerConvert Version 7.0 elérhetőségét. A megoldás kibővített többplatformos támogatással hozzásegíti a vállalatokat a kiszolgálói alkalmazások heterogén fizikai és virtuális IT környezetekben történő migrálásához és védelméhez. A vállalat 2008. márciusi felvásárlása óta a PlateSpin PowerConvert 7.0 az első jelentős fejlesztés, amely leegyszerűsíti az alkalmazások kezelését a heterogén adatközpontokban.

A Linux- és Windows-alapú alkalmazások kiterjedt támogatásával a PowerConvert új, lemezképalapú katasztrófa-helyreállítást és gyorsabb áttérést biztosít a nagy méretű telepítéseknél. A SUSE Linux Enterprise hatékonyabb támogatása mellett a PlateSpin PowerConvert nem csak a Red Hat Enterprise Linux rendszert támogatja, hanem a kulcsfontosságú, 64 bites Microsoft Windows Server-alapú alkalmazásokat és Citrix XenServer környezeteket is. A PlateSpin PowerConvert rugalmas adatközpont optimalizálást biztosít, mivel elválasztja a kiszolgálók alkalmazását az őket működtető hardvertől, és elosztja azt az egész hálózaton a fizikai kiszolgálók, blade infrastruktúrák, virtuális számítógépek és lemezképarchívumok között.

> A PowerConvert 7.0 új szolgáltatásai

- Linux-áttelepítés „bárhonnan-fizikai gépre”: Hatékony funkciók segítik az áttérést az egyik fizikai gépről a másikra (P2P) és virtuális gépről fizikaira (V2P), így a Linux alkalmazások átvihetők a fizikai és virtuális határokon a 32 bites Novell SUSE Linux Enterprise Server és a Red Hat Enterprise Linux rendszerekre. Ennek köszönhetően az ügyfelek felgyorsíthatják az adatközpont-kezdeményezéseket, beleértve a kiszolgálókonszolidációt, a hardverkölsönzéshez kapcsolódó áttéréseket és az adatközpontok áthelyezését.
- 64 bites Windows támogatása: 64 bites Windows átvitele fizikai gépről virtuálisra (P2V) a kulcsfontosságú Windows Server 2003 alkalmazásoknál, amely számos átviteli módszert támogat, beleértve az irányítás átvételét, a valós idejű fájlátvitelt és a pillanatképeket a VMware ESX 3.x, 3.5 és a Citrix XEN Enterprise 4.1 esetében. Így az ügyfelek egyetlen megoldással megvalósíthatják a hatékony átvitelt.
- A Citrix XenServer kibővített támogatása: Támogatja az alkalmazás átvitelét „bárhonnan- virtuális gépre” (X2V), illetve virtuális gépről lemezképfájlba (V2I) a Citrix XenServer Enterprise 4.1 környezetben a 32 bites Windows XP, 2000, 2003 és a 64 bites Windows Server 2003 esetén. Így az ügyfelek felgyorsíthatják és leegyszerűsíthetik az integrációt, és a lehető legjobban használhatják ki informatikai befektetéseiket.

A Plate Spin technológiája az IT-szakértők számára biztosítja
a heterogén adatközpont terhelés alapú nézetét,
ezáltal új lehetőségeket kínál a szervezetek számára
a hatékonyabb működéshez és a költségek csökkentéséhez.

- Jobb lemezképező funkciók: A rugalmas lemezképezés támogatása hatékonyabb alkalmazás-védelmet eredményez, és eközben jelentős megtakarításokat jelent mind munkaidőben, mind pedig a sávszélességben és a tárolási költségekben. A kiemelkedő lemezké-importhálózati és -exportálási funkciók, valamint az automatizálás lehetővé teszi, hogy a szervezetek könnyebben létrehozzák és kezeljék a kiszolgáló-alkalmazások lemezképalapú tárolását a biztonsági mentésekhez és a katasztrófa-helyreállításához, valamint csökkentsék a lemezképezéssel járó költségeket.
- Nagyvállalati sebesség és megbízhatóság – Drasztikusan nőtt az alkalmazás-átvitel sebessége a különböző hálózatokon, a Gigabit Ethernet hálózatoktól kezdve a nagy késleltetéssel működő WAN környezetekig. Ezen kívül mindenhol használhatóak a nagyvállalati alkalmazás-átviteli funkciók, például a kiszolgálószinkronizálási vagy a feladatautomatizálási és az átvitel utáni tesztelésre alkalmas szolgáltatások, amelyek a minimálisra csökkentik az állásidőt, és maximalizálják az alkalmazás-átvitel integritását. A PlateSpin PowerConvert nagyvállalati szintű megbízhatósága révén csökkenti az átviteli projektekhez szükséges időt és az üzleti kockázatokat, így hamarabb lesz eredményes a rendszer a nagy méretű adatközpontokban.

> Költséghatékony katasztrófa-helyreállítási megoldások a PlateSpintől kis- és középvállalatok számára

Az új, 2008. júniusában bejelentett PlateSpin Forge csomagok segítségével költséghatékonyan működtethető az innovatív katasztrófa-helyreállítási hardveralkalmazás az olyan kis- és középvállalatok számára, akiknél 10 vagy annál több kiszolgáló munkaterhelésének védelmét kell biztosítani.

A PlateSpin Forge egy célorientáltan kifejlesztett, összevont helyreállítási megoldás, amely előre csomagolt és beállított hardvert, szoftvert valamint virtualizációs technológiát tartalmaz a gyors telepítés, a testreszabás leegyszerűsítése illetve a teljes birtoklási költség csökkentése érdekében. A kis- és középvállalatok számára a 10, illetve 25 munkaterhelést védő modellt kínálják. Az új megoldásnak köszönhetően a helyreállítási befektetések költségei jobban illeszkednek az adatközpont méretéhez valamint a leállás vagy katasztrófa esetén védett fizikai vagy virtuális kiszolgálói munkaterhelések számához.

A kis- és középvállalatok piacán egyre nagyobb az igény a PlateSpin Forge termékhez hasonló, költséghatékony helyreállítási megoldások iránt, amelyek a virtualizáció segítségével egy virtuális gép bekapcsolásához hasonlóan egyszerűvé teszik a helyreállítást egy esetleges katasztrófa után. A virtualizált helyreállítási technológiák támogatják a távolabbi célokat és a stratégiai kezdeményezéseket is, amelyek


rugalmasabbá és könnyebben kezelhetővé kívánják tenni az informatikai környezeteket. A 10 munkaterhelésű PlateSpin Forge modell 5 munkaterhelésenként bővíthető, így rugalmasan követi a vállalkozás növekedését.

A PlateSpin Forge 10 munkaterhelésű modelljének megjelenésével a hivatalos PlateSpin viszonteladóknak az eddiginél több lehetőségük nyílik arra, hogy a kis- és középvállalatoknak megfizethető, azonnal üzembe helyezhető katasztrófa-helyreállítási megoldásokat valamint értéknovelt szolgáltatásokat nyújtsanak.

A teljes körű hardvert, szoftvert és tárhelyet tartalmazó egyszerűen használható adatvédelmi rendszer kiadásával a PlateSpin Forge jelentősen lecsökkenti a helyreállítási környezetek tervezéséhez, fenntartásához és telepítéséhez szükséges időt, valamint speciális technikai erőforrásokat. Így a kis- és középvállalatok a korábbi több hónapos időszak helyett, már napok alatt megkezdhetik alkalmazásaik védelmét.

A PlateSpin Forge tartalmaz egy új központi irányítókonzolt, amellyel egyszerűen kezelhető és „egyetlen ablakon” figyelhető akár több PlateSpin Forge alkalmazás is. Ez egyszerű felügyeletet tesz lehetővé, melynek köszönhetően a felhasználó biztonságban tudhatja alkalmazásait egy esetleges áramkimaradás esetén.

A Novell vállalata, a PlateSpin egységes megoldáscsomagot kínál a vállalatoknak az adatközponti kiszolgálóvirtualizálás bevezetéséhez, felügyeletéhez és bővítéséhez. A PlateSpin technológiája függetleníti az alkalmazást a hardverplatformtól, lehetővé téve az adatok, alkalmazások és operációs rendszerek hálózaton belüli mozgatását a fizikai vagy virtuális gépek között. A kiszolgálók alkalmazásának fizikai és virtuális környezetekben történő hordozhatóságának, védelmének, kiosztásának és optimalizálásának köszönhetően a vállalatok csökkenthetik a költségeket, a rendszer bonyolultságát és a kockázatokat. Az alkalmazás beépített profilképzése és tervezése segítségével a PlateSpin megoldásai javítják az adatközpont-kezdeményezésekkel elérhető sebességet és minőséget, így megkönnyítik a heterogén informatikai környezetek felügyeletét.

Reméljük, hogy a PlateSpin termékek részletes bemutatását követően Ön szerint is érdemes elgondolkozni azon, hogy milyen módon lehet bevezetni ezeket a megoldásokat az Ön IT-környezetébe az adatközponti kezdeményezések sebességének és minőségének javítása érdekében. A PlateSpinnel kapcsolatos további információért, illetve a termék letöltéséhez, kipróbálásához vagy megvásárlásához látogasson el a platespin.com oldalra. 

„Aki mások nyomában jár, sohasem kerülhet elébük.”
–Michelangelo–

Ma már elképzelhetetlen a kommunikáció mobil készülékek nélkül - de vajon biztonságosan használjuk őket?

Biztonság már a mobil végpontokon is

Frissítés NetWare-ről?

A funkciókban gazdag Open Enterprise Server 2 előnyei a Windows Serverhez képest

TECHNOLÓGIA



Biztonság már a mobil végpontokon is



Ma már elképzelhetetlen a kommunikáció mobil készülékek nélkül – de vajon biztonságosan használjuk őket?

Avilág folyamatosan változik és az információbiztonsággal kapcsolatos munkának valójában soha sincs vége. Ez annak köszönhető, hogy gyakorlatilag fegyverkezési versenyben állunk a számítógépes bűnözőkkel. Folyamatosan változnak az üzleti prioritások és folyamatok, és ezek változásával egyidőben változniuk kell a biztonsági intézkedéseknek is. Az üzleti folyamatok egyik biztonsági környezetet is átformáló változása a mobilitás terjedése. Korábban a cég központjában egy nagyszámítógépen vagy szerveren tárolt adatokat most laptopok ezrein tárolják. A hálózat régen statikus kábelek kötegeit jelentette, most a vezeték nélküli kapcsolatoknak köszönhetően dinamikusan változik. A kiszámítható hálózati útvonalakon áramló adatok a hálózati figyelő- és felügyeleti eszközök számára észrevétlenül most sok gigabájtos, apró méretű USB-meghajtókon cserélnek gazdát.

Ezek a változások azt jelentik, hogy a régi típusú biztonsági megoldások nem elegendőek többé. Szükség van rájuk, de nem jelentenek megfelelő védelmet az új generációs fenyegetések ellen. Amiatt is aggódni kell, hogy megpróbálnak betörni a hálózatba és ellopják a szerverről a kritikus fontosságú adatokat. De mi van ezeknek az adatoknak a vezetők céges gépein található változatával? Mi értelme van egy jól működő peremtűzfalnak, ha a laptopot a taxiban felejtik vagy WiFi hot-spot nem biztonságos hálózatán használják?

> Az új problémákhoz új megoldások kellenek

A hagyományos biztonsági intézkedéseket olyan új megoldásokkal kell kiegészíteni, amelyek közvetlenül az új fenyegetéseket veszik célba. Ezért vásárolta fel a Novell a Senforce Technologies-t, és ezért is jelent meg ZENworks Endpoint Security Management termék.

A ZENworks Endpoint Security Management lehetőséget biztosít a biztonsági rendszergazdáknak a végpontokra (például munkaállomásokra és laptopokra) vonatkozó céges biztonsági irányelvek központi meghatározására, valamint ezek állandó és folyamatos kikényszerítésére. A kikényszerítés kernelszintű illesztőkkel történik, így akkor sem sérül a biztonság, ha a számítógép lekapcsolódik a hálózatról, vagy nem használják. A céges irányelvek kikényszerítésének és a központosított felügyeletnek az előbbieken leírt kombinációja rendkívül fontos a megfelelő kockázatkezeléshez. Abban az esetben, ha a felhasználók maguk hozzák meg a saját biztonságukra vonatkozó döntéseket, jónéhány problémával kell majd

szembesülniük a rendszergazdáknak:

1. Gyakran kell megzavarniuk a felhasználót feladatai teljesítése közben.
2. El kell érni, hogy a felhasználó amatőr biztonsági szakemberré váljon, ami elkerülhetetlenül azt jelenti, hogy rossz döntések is születnek majd.
3. Nem lehet megvalósítani az egységességet a cégen belül, nem biztosítható az előírásoknak való megfelelés.

> A szolgáltatások hatóköre rendkívül fontos

Mivel a mobilitás nem csak műszaki kérdés, hanem alapjaiban változtatja meg a technológia használatát, ezért biztonsági kérdések egész sorát veti fel. A ZENworks Endpoint Security Managementet úgy tervezték, hogy többféle kikényszerítési mechanizmust kínáljon egyetlen integrált felügyeleti keretrendszeren belül, amelyeket egyetlen ügynökprogram hajt végre. Ezek a mechanizmusok az alábbiak:

1. rendkívül részletesen ellenőrzik a bejövő és kimenő csomagok áramlását egy végponti tűzfal használatával,
2. mindenre kiterjedő felügyeletet látnak el a vezeték nélküli használat fölött, például lehetőséget adnak a rendszergazdák számára:
 - a vezeték nélküli használat teljes letiltására
 - a hozzáférési pontokról szóló fehér lista készítésére (hogy ne véletlenszerűen történjen a felkapcsolódás), vagy
 - minimális titkosítási normák kikényszerítésére (például hogy elfogadható minimumként követelje meg a WPA használatát és utasítsa el a WEP-et),
3. biztosítják a hordozható eszközök átfogó felügyeletét, így a rendszergazdáknak lehetősége nyílik az ilyen eszközök teljes tiltására, az engedélyezett fehér listába sorolására, illetve csak az olvasási használat engedélyezésére,
4. úgyszintén lehetőséget adnak a hordozható eszközre kiírt adatok automatikus titkosításának kikényszerítésére és/vagy a merevlemezben tárolt adatok titkosítására a fájl-/könyvtárinformációk alapján,
5. a rendszergazdák kikényszeríthetik a felhasználóktól a vállalati VPN használatát,
6. a rendszergazdák lehetőséget kapnak arra, hogy kézben tartsák, mely alkalmazásokat lehet végrehajtani a végpontokon,
7. lehetőség nyílik a ZENworks Security Client használatára annak érdekében, hogy a biztonsági eseményekre automatikus válaszokat adhasson a rendszer, hogy rendszergazdai beavatkozás nélkül valós idejű, parancsfájlokkal meghatározott műveleteket hajthasson végre válaszul,

**Mindezek a változások azt jelentik,
 hogy a régi típusú biztonsági megoldások
 (mint például a peremtűzfalak és a peremhálózati vírusellenőrzők) nem elegendőek többé.
 Még mindig szükség van rájuk,
 de nem jelentenek megfelelő védelmet az új generációs fenyegetések ellen.**

8. irányelvekkel vezérelhető lesz az összes fizikai port és protokoll működése (Bluetooth, IrDA, soros és párhuzamos port, modemek stb.)
 Ezek a szolgáltatások valós időben működnek és nincs szükségük a felhasználó beavatkozására.

> Hogy működik mindez?

Az architektúra

A megoldás több különböző elemet tartalmaz. Amint az 1. ábrán is látható, ezek az alábbiak:

ZENworks Security Client: A ZENworks biztonsági kliens az az ügynökprogram, amely a végpontokon kikényszeríti a biztonsági intézkedéseket. Ez a biztonság „karja”, míg a központilag létrehozott irányelvek alkotják az „agyat”.

Policy Distribution Service: Az irányelv-szétosztási szolgáltatás felelős a biztonsági irányelvek eljuttatásáért a ZENworks Security Client-ekhez, és ez fogadja a kliensek jelentési adatait is. Az irányelv-szétosztási szolgáltatás telepíthető a demilitarizált zónában (DMZ), a vállalati tűzfalon kívül a mobil végpontok rendszeres irányelv-frissítéseinek biztosításához. Ez azt jelenti, hogy a kliensek LAN-kapcsolat nélkül is frissíthetők.

Management Service: A felügyeleti szolgáltatás a hálózat egy biztonságos pontján található. Felelős a felhasználói irányelvek társításáért, az összetevők hitelesítéséért, a jelentési adatok beolvasásáért, a jelentések készítéséért, illetve a tárolási és biztonsági irányelvek létrehozásáért.

Management Console: A felügyeleti konzol a rendszergazdák által használt felhasználói felület, amely vagy közvetlenül a felügyeleti szolgáltatást futtató szerveren fut, vagy egy másik munkaállomáson, amely biztonságos hozzáféréssel rendelkezik a felügyeleti szolgáltatás szerveréhez. A felügyeleti konzolt a felügyeleti szolgáltatás beállításához, a felhasználói és csoportirányelvek létrehozásához és felügyeletéhez használják. Az irányelvek létrehozhatók, másolhatók, szerkeszthetők, szétoszthatók vagy törölhetők.

Client Location Assurance Service: A kliens helyét ellenőrző szolgáltatás – melynek használata nem kötelező – titkosított módon garantálja, hogy a ZENworks Security Client valóban a megadott helyen található. További részletek a későbbi Hely, hely, hely bekezdésben.

Irányelvek létrehozása és szétosztása

Az irányelvek létrehozására a felügyeleti konzol használható. Ez egy egyszerű grafikus felület a rendszergazdák biztonsági igényeinek megadásához. Ha például el szeretné kerülni azokat a fenyegetéseket, amelyek abból származnak, hogy a felhasználók egyidőben csatlakoznak vezetékes és valamilyen más – esetleg veszélyes – vezeték nélküli hálózatra, egyszerűen jelölje meg a „no wireless when wired” (vezeték nélküli hálózat letiltása, ha van vezetékes) lehetőséget. Az irányelv-szétosztási szolgáltatás igénybevételel történő felügyelet során, az irányelvek egy XML BLOB állományban gyűlnek össze, amit a rendszer tömörít, AES-256 kódolással titkosít és digitálisan aláír, mielőtt szétküldené a végpontokra.

Hogy működik az ügynökprogram?

A végpontokon a kikényszerítést első sorban kernelszinten működő illesztők végzik. A végpont tűzfala például egy hálózati illesztőfelület-specifikációs (Network Driver Interface Specification, NDIS), köztes miniport-illesztőt használ arra, hogy a csomagokat egy alacsony hálózati réteg szintjén szűrje. A ZENworks Security Client hatékony, biztonságos csomagszűrést biztosít azzal, hogy a csomagokat azonnal elfogja, amint feljebb érnek a hardverabsztrakciós rétegből. Az architektúra kliensen belüli előnye az is, hogy a kernelszintű illesztők a felhasználó által generált forgalom kívül látják azt a belső felügyeleti forgalmat is, amit az operációs rendszer használ az alapvető szolgáltatásokhoz. Az olyan vezetékek nélküli funkciók, mint a látható hozzáférési pontok „bejárás táblája” keresztülhalad a kernel ZENworks Security Client által felügyelt részein, és az ügynök szűrheti ezeket az irányelvben található fehérlista szerint. Ezzel a rendszergazdák könnyen kézben tarthatják, hogy a felhasználók melyik hozzáférési pontokhoz csatlakozhatnak, amely jelentősen csökkenti a véletlen kapcsolódások okozta veszélyeket. Mivel a szűrés kernelszinten, nem pedig alkalmazásszinten történik, a szűrés minden vezeték nélküli felügyeleti alkalmazásnál működik (lásd 1. ábra).



1. ÁBRA: A ZENworks Endpoint Security Management központilag meghatározott irányelveket szállít és aktívan betartatja azokat a végpontokon – függetlenül azok helyétől

A hálózati szinten működő illesztők nem tudnák a korábbiakban leírt összes biztonsági kényszerítő intézkedést végrehajtani. A ZENworks Security Client számos más illesztőt is használ, amelyek a fájlrendszer szintjén fejtik ki tevékenységüket, például adattitkosítást végeznek, vagy ellenőrzik a hordozható eszközök titkosítását. A ZENworks Endpoint Security Management terméknek is vannak mobil adathordozókra vonatkozó biztonsági funkciói.

Nagyvállalati működés

A ZENworks Endpoint Security Management a nagyvállalati piacra készült termék számos olyan funkciójával rendelkezik, amely növeli a hatékonyságot és teljesítményt. Ilyen funkciók például az alábbiak:

1. Felhasználókra vagy gépekre vonatkozó irányelvek. Nem lehet olyan „konfekció”-irányelveket készíteni, amelyek

Fontos, hogy a biztonsági beállításokat központilag lehessen megadni és felügyelni.

Ellenkező esetben még csak nem is állíthatja, hogy vannak biztonsági irányelvek: csak néhány jó cél van és néhány rosszul használt biztonsági eszköz.

minden cégnek egyformán megfelelőek. A vezetők munkaprofilja (és fenyegetési profilja) alapjaiban eltér a támogatási csoport munkatársaitól, mint ahogy a kereskedőké is a belső informatikai rendszert biztosítótól. Amire szükség van – és amire a ZENworks Endpoint Security Management lehetőséget ad – az az, hogy különböző irányelveket lehessen létrehozni az egyes felhasználóknak, majd ezeket az irányelveket a megfelelő szereplőkhöz lehessen hozzá rendelni. Ehhez a ZENworks Endpoint Security Management hozzákapcsolódik a vállalati címtárhoz (akár eDirectoryról, Active Directoryről vagy bármilyen más LDAP-kompatibilis személyazonosság-tárról van szó) és lehetőséget ad az irányelvek megfelelő célokhoz rendelésére, az egyedi felhasználók, a csoportok vagy szervezeti egységek, illetve a személyazonosság-konténerek bármilyen más szintjén. Az irányelvek akár gépekre is irányulhatnak a felhasználók helyett, így könnyebben megvalósítható a biztonsági felügyelet a megosztott gépeken.

2. Kiforrott jelentéskészítési és felülvizsgálati szolgáltatások. Fontos, hogy a biztonsági kikényszerítést ne lehessen „beállítani majd elfelejteni”. A kényszerítő intézkedéseket magas szinten méretezhető jelentéskészítési és felülvizsgálati mechanizmusokkal kell támogatni.

Megadható, hogy melyik jelentéseket szeretné látni, ekkor a ZENworks Security Client a Distribution Service eszközt használva létrehozza a megfelelő jelentési adatokat és visszaküldi ezeket a felügyeleti szerverre. Az adatokat ezután a felügyeleti szerver összegyűjti, elemzi, és összeállítja belőlük a kívánt jelentéseket.

3. Erős kliens-önvédelmi funkciók. Ha a vállalat komolyan gondolja az előírások betartását, akkor fontos, hogy a felhasználók ne tudják azt megkerülni vagy kikapcsolni a kényszerítést. Az ezzel kapcsolatos problémákat a ZENworks Security Client úgy előzi meg, hogy hatékonyan hárítja el a felhasználók támadásait, még akkor is, ha a kérdéses gépen adminisztrátori jogosultságokkal rendelkező felhasználókról van szó. A rendszer valós időben észleli a folyamatok leállítására, az illetzők eltávolítására vagy a rendszerleíró adatbázis megváltoztatására tett összes kísérletet, így védelmet nyújt az adminisztrátori műveletek ellen és naplózza azokat.

Kiforrott technológia


Az emberek méltán lesznek idegesek, ha az „új kernelszintű illesztőtechnológiáról” hallanak. Ez olyan, mint amikor az orvos azt mondja: „Ez a LEGELŐ alkalom, hogy ezt a műtetet valakin elvégezzük”. Az új technológia előnyeinek kihasználása egy dolog, kísérleti nyúlnak lenni egy másik. Ne felejtse el azonban, hogy a ZENworks Endpoint Security Management egy már beérett, a piac által kipróbált technológia, amely a Senforce Technologies felvásárlásával került a Novell portfóliójába. A termék négy éve van a piacon, és széles körben használják.

> Hely, hely, hely

Folytatjuk azt a gondolatmenetet, hogy nincs olyan alapértelmezett irányelv, amely a cég összes dolgozójának megfelelné. A biztonság maximalizálása és a termelési költségek csökkentése érdekében sokszor nincs más alternatíva, mint hogy számos különféle irányelvet kell létrehozni és ezeket különféle csoportokhoz kell rendelni.

Mivel mobil világban élünk, a helyzet még ennél is összetettebb. Még egy adott személy esetében sincs igazán olyan irányelv, amely mindig megfelelné. A ZENworks Endpoint Security Managementet a mobil munkaerő igényeinek megfelelően fejlesztették ki, emiatt a termék irányelvei (és irányelv-kikényszerítése) helytudatos módon épülnek fel. A rendszergazdák készíthetnek olyan irányelveket, amelyeknek a végponton egy adott hálózati helyen kell érvényre jutniuk. A hálózati paraméterekre (például IP-címekre, alapértelmezett átjárókra, DHCP-szerver címekre stb.) teljes rálátással rendelkező ügynökprogram azonosítja, hogy jelenleg melyik hely használható és alkalmazza az adott környezetre érvényes biztonsági irányelveket. Így a rendszergazdák egyszerűen készíthetnek olyan irányelveket, amelyek azt mondják, hogy „ha a felhasználóim a céges helyi hálózatot használják, akkor engedélyezem a hálózati forgalmat, de ha egy internetkávézóban ülnek, akkor ezeknek a portoknak az állapota inkább legyen 'stateful' (állapotfigyelő), ne 'open' (nyitott)”. A helytudatos működés teljes egészében automatikus, nem igényli a felhasználó beavatkozását.

> Összefoglalás

A világ megváltozott, és a régi típusú biztonsági intézkedések, mint például a peremtűzfalak és a peremhálózati vírusszűrés már nem elegendőek. Ma már a mobil eszközökön is közvetlenül ki kell kényszeríteni a biztonsági intézkedéseket. Miközben ezt a kikényszerítést elosztottan kell végezni, rendkívül fontos, hogy a biztonsági irányelvek felügyelete és meghatározása központilag történjen. A ZENworks Endpoint Security Managementet a mobil munkaerő igényeinek megfelelően fejlesztették ki. Használatával a biztonsági rendszergazdák a konzol előtt ülve kijelenthetik hogy a „céges irányelvek azok, amelyeket a felhasználóknak be KELL tartaniuk”, és hogy az irányelveket biztonságosan szétosztották az összes felhasználónak és valóban ki is kényszerítették ezek használatát. Nem számít, hogy a problémát a csomagok hálózaton keresztül történő áramlása jelenti, mert a vezeték nélküli használat biztonságossá tétele, a hordozható média-felügyelet vagy az érzékeny adatok titkosítása – melyeket a rendszergazdák mind-mind ellenőrzésük alatt tarthatnak – egyetlen egységes felügyeleti és jelentéskészítési keretrendszerből megoldhatók. 

Frissítés NetWare-ról?

A funkciókban gazdag Open Enterprise Server 2 előnyei a Windows Serverhez képest



Amikor a Novell ügyfelek azt fontolgatják, hogy NetWare környezetüket a Linuxon futó Novell Open Enterprise Serverre állítják át, néhányan úgy gondolják, hogy a megfelelő körütekintéssel meghozott döntéshez más átállási lehetőségeket is számításba kell venniük. Ezek az egyéb átállási lehetőségek jellemzően a Windows Server 2008-at vagy a Windows Server 2003-at jelentik. A Novell által készített tanulmány segítséget nyújt a lehetőségek kiértékelésében, és bemutatja a Linux platformon futó Novell Open Enterprise Server 2-re, illetve a Windows Server környezetre történő átállás legfontosabb tényezőit: összehasonlítja az átállási folyamatokat, de szó esik a tervezésről és a telepítésről, az oktatási igényekről, a műveleti hatékonyság növekedéséről vagy csökkenéséről, a viszonylagos költségmegtakarításokról és költségekről, valamint a potenciális kockázatokról. A tanulmányban szereplő adatok a valós ügyféltapasztalatokból, a Novell Consulting által vezetett kutatásból, valamint a Novell és Microsoft szerverplatformokat egyaránt telepítő viszonteladóktól származnak, a tényleges eredmények ügyfelenként eltérőek lehetnek.

> A Windows Server 2008 termékkel kapcsolatos általános megfontolások

Sokat hallhatunk a Windows Server 2008 legfrissebb kiadásáról, de nem sok konkrétumot tudni a Microsoft ajánlatáról. Növelni fogja-e a biztonságot, a stabilitást és a teljesítményt, ahogy a Microsoft-vásárlók remélik? Előrelépést jelent-e a Windows Server 2003-hoz képest, vagy gyakorlatilag ugyanaz lesz mint az előző változat? Talán hasonló lesz a Windows Vista kiadáshoz, amiről vegyes értékelések születtek, és amelyet néhányan egyértelmű visszalépésnek látnak? Vajon megfelel-e a vásárlók elvárásainak és elégedetté teszi-e őket legalább olyan mértékben, mint azt a Novell esetében megszokták? Egyelőre még túl korai ítéletet mondani a Windows Server 2008-ról, az azonban egyértelmű, hogy a termék olyan kernelmódosításokat tartalmaz, amelyek telepítése előtt kiterjedt alkalmazástesztelés szükséges. Ez késleltetheti a szoftvergyártók tanúsítványainak megjelenését is.

A fenti problémákat azok az elemzők is megerősítik, akik szerint a cégeknek legalább 18 hónapra lesz szükségük a pilot tesztek elvégzéséhez, az alkalmazások kompatibilitásának ellenőrzéséhez, új rendszerkép-könyvtárak felépítéséhez valamint a személyi állomány betanításához. Ezek a telepítést

megelőző feladatok legalább 2009-ig megakadályozzák a legtöbb szervezetet a bevezetésben. A teljes átállás sok esetben még ezek után is évekig tarthat, különösen azoknál a nagyvállalatoknál, amelyeknél az átállás világszerte több száz szervert érint.

A Novell Open Enterprise Server 2 és a Windows Server 2008 összehasonlításakor kiderül, hogy a Novell Open Enterprise Server 2 fejlettebb funkciókészlettel rendelkezik, amelyben megtalálható többek között a tárolóvirtualizáció (Dynamic Storage Technology), a szervervirtualizáció és a felhasználók önkiszolgáló adminisztrációjának lehetősége.

> A Windows Server 2003-ra történő átállás növeli a költségeket és fokozza a veszélyeket

A NetWare rendszerről Windows Server 2003-ra végzett átállás több pénzt és munkát igényel, mint a Novell Open Enterprise Server 2-re történő frissítés. A költségek nagy része a Windows Server használatához szükséges jelentős hardverberuházásokkal függ össze, de további költséget jelent a rendszergazdák és helpdesk-munkatársak oktatása is. Míg a Novell Open Enterprise Serverre történő átálláskor a folyamatok nagy része automatizált, a Windows Serverre való átállás jelentős része manuális.

> Nagyobb szerverhardver-befektetések

A kutatásban olyan megoldásszállítók vettek részt, akik mind a Novell Open Enterprise Server, mind a Windows Server 2003 telepítésében járatosak. Véleményük szerint a szerverhardver beszerzésekor jelentős költségmegtakarítást eredményez, hogy a linuxos Novell Open Enterprise Server ezernél is több fájl- és nyomtatási felhasználót képes kiszolgálni. A Windows Server 2003 esetében nem csak a fájl- és nyomtatási szolgáltatások biztosításához van szükség több szerverhardverre, hanem az egyéb Microsoft hálózati szolgáltatásokhoz is, amely a költségek további növekedését eredményezi.

A hardverbeszerzés és -karbantartás költségeinek vizsgálata során sok cég szembesülhet azzal, hogy dollárszázereket takarítanak meg a linuxos Novell Open Enterprise Server környezetre történő frissítéssel a Windows Server 2003-ra való átállással szemben. A hardverbeszerzési különbség még nagyobb, főleg, ha a szervervirtualizációt is számításba vesszük.

A vásárlók és a partnerek szerint a NetWare – Windows Server 2003 átállás megtervezéséhez legalább kétszer annyi időre van szükség, mint az Open Enterprise Serverre frissítés megtervezéséhez.

> SAN-duplikáció és a tárolóterület megkétszerezése

Ha a NetWare környezetben SAN is működik, akkor még nagyobb hardverköltséggel kell számolni a Windows Server 2003-ra való átállásnál. A SAN Windowsra történő áthelyezésénél a legtöbb esetben nem elegendő egy kisebb tömböt létrehozni a SAN-on, áttenni a Windows-oldalra, majd lekapcsolni a NetWare-oldalt, és addig ismételni ezt a műveletet, amíg az egész át nem kerül.

Egy SAN Windows Server 2003-ra való átállításkor egy teljes logikai egység számot (LUN-t) kell egyidőben áttenni. Mivel a legtöbb szervezet egyetlen LUN-ra állította be a teljes SAN-t, az egészet egyszerre kell áthelyezni, tehát az átállás előtt léteznie kell egy teljes funkcionalitású forrás- és cél-SAN-nak - ehhez pedig meg kell vásárolni és telepíteni kell egy teljes új SAN-t, célrendszerként. A Storage Performance Council költség számításai alapján egy átlagos SAN-beszerzés költsége 125 USD/GB. Egy 10 terabájtos SAN-t tekintve ez minimum 1 millió 250 ezer dolláros beszerzési költséget jelent, és ebben még nincsenek benne a telepítés és a hely kialakításának költségei. A SAN-rendszer windowsos átállításának költségei mellett további kiadásokkal is számolni kell a Windows Server 2003 alapszintű tárolási igényei miatt. A vásárlókkal és a megoldásszállítókkal folytatott konzultáció alapján megduplázhathja a tárolóigényt az adatok áthelyezése NSS-kötetekről a Windows Server NTFS-köteteire.

> Kézi vagy automatikus átállás?

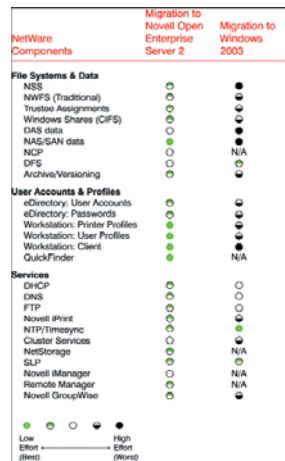
A Windows-környezetre való átállás a szükséges hardverberuházások mellett sokkal több időt és munkát is igényel, mint a NetWare frissítése a Novell Open Enterprise Server 2-re. Ez utóbbi egy világos és egyértelmű, automatizált művelet, ami lényegében észrevehetetlen a végfelhasználók számára. A Windows Server 2003-ra történő átállás legnagyobb része azonban manuálisan történik, és bizonyos esetekben a végfelhasználók közreműködése is szükséges a befejezés előtt.

A Novell eDirectory fiókok linuxos Novell Open Enterprise Server 2 platformra történő átviteléhez egy kis előkészítő munkára van szükség, például el kell végezni az állapotellenőrzéseket és naprakész állapotba kell hozni a fákat egy automatikus szinkronizációs folyamat használatával. Ahhoz azonban, hogy ezeket a felhasználói fiókokat az Active Directoryba vigyük át, jelentős előzetes tervezésre és az AD-tartomány szerkezet kialakítására van szükség. A fiókok átvitele elsődlegesen manuálisan történik és rendkívül időigényes. Minden asztali rendszert manuálisan be kell léptetni az Active Directory tartományokba, és a felhasználóknak újra be kell írniuk saját jelszavukat.

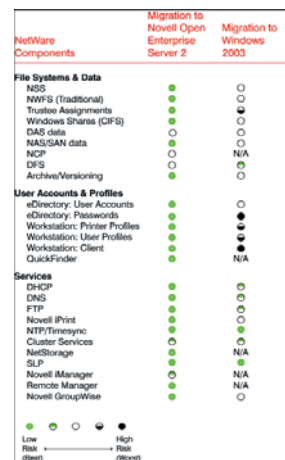
Sok példa van arra, hogy milyen eltérő feladatokat igényel a két célrendszerre való átállás. Egy NetWare NSS-tárolókötet

átállítása a SAN-on Linuxra mindössze annyit jelent, hogy le kell kapcsolni a NetWare-en és felkapcsolni a Linux-rendszeren. Ezzel szemben egy SAN Windows Server 2003-ra történő átállítása jelentősen több időt és munkát igényel.

A Windows Server 2003-ra való átállás manuális feladatai közé tartozik a cég minden egyes munkaállomásának átállítása, a Novell-kliens törlése és a nyomtatóprofilok ismételt létrehozása. Ezekhez szükség van az összes asztaligép- és noteszgép-rendszerkép frissítésére. Emellett egy Windows Server 2003 átállás nem csak jelentős mennyiségű időt és erőforrást emészt fel, de a manuális munka miatt jelentős kockázatokat is jelent, mivel benne van az emberi hibák lehetősége is.



1. ÁBRA: A szükséges erőforrások NetWare komponensek Novell Open Enterprise Server 2-re, illetve Windows Server 2003-ra történő migrálásához. Zöld – könnyű, fekete – bonyolult



2. ÁBRA: Összehasonlítás: kockázatok a NetWare komponensek Novell Open Enterprise Server 2-re, illetve Windows Server 2003-ra történő migrálása során

> A Novell Open Enterprise Server 2 szolgáltatásai

Ha azt fontolgatja, hogy a NetWare rendszerről Novell Open Enterprise Server 2 vagy Windows Server környezetre áll át, az átállás költségeinek és nehézségeinek figyelembe vétele mellett érdemes más tényezőket is megvizsgálni. A NetWare-ről Windows Serverre való átállás nem eredményez funkcionálisan egyenértékű megoldást, így csökkenti a műveleti hatékonyságot és növeli az adminisztrációs költségeket. A linuxos Novell Open Enterprise Server 2 platformra frissítés jelentős műveleti és pénzügyi előnyökkel jár, különösen a tárolóvirtualizáció (Dynamic Storage Technology), a szervervirtualizáció és a felhasználók önkiszolgálási lehetőségei terén. A végeredmény: a Windows Serverre történő átállás azonnali jelentős költséget jelent és növeli a folyamatos informatikai kiadásokat. Emellett csökkenti a műveleti hatékonyságot és használata számos kockázattal jár. A Novell Open Enterprise Server 2-re való átállás ugyanakkor komoly megtakarításokat eredményez, növeli a hatékonyságot és a termelékenységet, valamint minimalisra csökkenti a kockázatot.



3. ÁBRA: A Novell Open Enterprise Server minden idők legtöbbet tudó NetWare és egyben Linux szervere

Open Enterprise Server 2 - SUSE Linux alapú munkacsoport szerver

A nemrégiben megjelent Open Enterprise Server 2 a nyílt és zárt forráskódú rendszerek legjobb tulajdonságait egyesítő SUSE Linux alapú munkacsoport kiszolgáló.

- N-** A „legtöbbet tudó” és legkönnyebben felügyelhető Linux szerver
- N-** Az összes hagyományos NetWare szolgáltatás SUSE Linux alapon
- N-** Egyszerű átállás NetWare-ről Linuxra
- N-** Kompatibilitás a régi alkalmazások számára
- N-** Dinamikus tárterület kezelés az üzletkritikus és a nem kritikus adatok kiválasztására
- N-** Beépített virtualizáció NetWare, Linux és Windows szerverek hatékony futtatására

A Novell Open Enterprise Server egy biztonságos, kiváló rendelkezésre állású megoldás, amely lehetőséget teremt arra, hogy a cégek a Linux-rendszereket csoportmunka és hálózati infrastruktúráként használják. A megoldás egyaránt működik SUSE Linux Enterprise Server és NetWare platformon, lehetővé téve a hálózati, kommunikációs és munkacsoportos szolgáltatások egyszerű telepítését mindkét platformon – vagy akár a kettő együttesen – a szervezet igényeinek megfelelően.

Alkalmazások széleskörű támogatása

A Novell Open Enterprise Server alapja a SUSE Linux Enterprise Server – az üzleti alkalmazások

vezető nyílt platformja, a piac legbiztonságosabb Linux-rendszere. Számos alkalmazásfejlesztő és rendszergyártó – így például a Dell, HP, IBM, Oracle és az SAP – minősítette rendszerét ehhez a kiforrott platformhoz, valamint nyílt forráskódú alkalmazások ezrei kompatibilisek ezzel az élvonalbeli Linux környezettel.

Hozzáadott érték a Linux mellé

A különféle integrált Novell-technológiákkal – a Novell eDirectory, a Novell iFolder, az iManager, az iPrint, a Novell Identity Manager, a ZENworks Linux Management, hogy csak a legfontosabbakat említsük – a Novell Open Enterprise Server az alábbi területeken egészíti ki a Linuxot: méretezhető felügyelet, globális biztonság, nagyfokú termelékenység, gyors telepítés.

Vegyes forráskódú rendszer a nyílt vállalat számára

A Novell Open Enterprise Server leginkább szembeűnő jellemzője a Novell által biztosított kiemelkedő támogatási szolgáltatások széles köre:

- N-** gyakorlati oktatások és minősítések,
- N-** teszteszabott konzultációs szolgáltatások,
- N-** folyamatos oktatás,
- N-** személyre szóló, mindig rendelkezésre álló műszaki támogatás,
- N-** hardver- és szoftverpartnerek széles köre,
- N-** ügyfélorientált tervezés és megoldásszállító partnerek az egész világon.

> Összegzés

Tendencia, hogy a felhasználók operációs rendszereiket egy konszolidációs folyamat keretében a két fő operációs rendszerre, a Linuxra, vagy a Windowsra állítják át. A SUSE Linux alapú Novell Open Enterprise Server 2 jelenleg az egyetlen kapocs a jövő két vezető operációs rendszere között. A Novell az egyetlen egymilliárd dolláros vállalat, amely saját Linux disztribúcióval és a köré épülő világméretű szakmai háttérrel rendelkezik, teljes termékportfóliója elérhető Linuxon is, a desktoptól az adatközpontokig. A Novell SUSE Linux jelenleg az egyetlen Microsoft által támogatott vállalati Linux disztribúció, és csak a Novell és a Microsoft ajánlanak közös technológiai támogatást ezen a területen.

Az informatikai részlegek számára napjaink egyik legnagyobb kihívása, hogy az egyre csökkenő költségvetés mellett elegendő legyenek a növekvő üzleti igényeknek. Ennek megoldására a Novell egyesíti a SUSE Linux Enterprise Server megoldását a Novell Open Enterprise Server termékbe szorosan integrált, bevált hálózati szolgáltatásokkal. A Novell Open Enterprise Server a Novell NetWare szolgáltatásainak linuxos alapokon való biztosításával lehetővé teszi a NetWare-felhasználók számára a Linuxra történő zökkenőmentes átállást. Az Open Enterprise Server 2 az összes NetWare munkacsoport-szolgáltatást már teljes egészében linuxos platformon biztosítja. A termék további újdonságai, mint a virtualizáció, a megnövelt alkalmazás- és hardvertámogatás, valamint az új tárolási szolgáltatások pedig egy Linux alapú, nyílt és biztonságos környezetben garantálják az együttműködést és a nagy rendelkezésre állást a vállalati szintű számítástechnikai igények kielégítéséhez. A Novell Open Enterprise Server tárolási szolgáltatásait az iparág vezető szállítók termékei is támogatják: az adatmentési megoldásszállítók közül a CA Arcserve, a Syncsort Backup Express, a Galaxy CommVault, a Symantec Netbackup és a Backup Exec, továbbá a Portlock Storage Manager for Linux, az EMC Legato Networker, az IBM Tivoli és a Bakbone NetVault, a vírusvédelmi megoldásszállítók közül pedig a McAfee Linux Shield, Trend Micro Server Protect, a Symantec AV, a Sophos Anti Virus, és az eTrust Antivirus. **N**



Informatikai rendszerfejlesztésének következő állomása: Az informatikai események valós idejű elemzése **A Novell Sentinellel**

Állítson egy mindig éber „őrszemet” informatikai rendszeréhez

- ➔ Tegyen eleget az IT-biztonsági megfelelési követelményeknek (SOX, PCI-DSS, PSZÁF, stb.), és kovácsoljon előnyt a kötelező logelemzés eredményeinek elemzéséből
- ➔ Észlelje valós időben a külső és belső fenyegetéseket, és oldja meg a problémákat még azok felmerülése előtt
- ➔ Használjon egy olyan rendszert, amely pontosan megmutatja, mikor mi történik informatikai rendszerében: az emberi erőforrásokat, a rendszereket és folyamatokat egyszerre felügyeli

Dőljön hátra, mert biztos lehet abban, hogy bizalmas adatai tökéletes védelmet kapnak!

