

Privileged User Manager

A rendszeradminisztrátorok sokáig korlátlan hatalommal rendelkeztek a teljes informatikai infrastruktúra felett. De megengedheti Ön akár egyetlen embernek is, hogy bármit megtehessen a szerverein? A NetIQ Privileged User Manager segítségével részletesen kidolgozott korlátok közé szoríthatja és folyamatosan ellenőrizheti a rendszeradminisztrátorok munkáját, megelőzheti a visszaéléseket, azonosíthatja az elkövetett hibák felelőseit, és bizonyíthatja az előírásoknak való megfelelést.

Csökkentse a kockázatot a felhatalmazás korlátozásával

A rendszeradminisztrátori jogosultságot biztosító felhasználói fiókok korlátlan hatalommal ruházzák fel a fiók jelszavát ismerő alkalmazottakat. Amennyiben egy hálózaton vagy szerveren többen is végeznek olyan feladatokat, melyekhez emelt szintű jogosultságok szükségesek, ezt sokszor a rendszeradminisztrátori fiók jelszavának egymás közötti megosztásával oldják meg. Így azonban a jelszót ismerők lényegében bármit megtehetnek és bármilyen adathoz hozzáférhetnek. Hiba vagy visszaélés esetén nehéz a felderítés, a felelős személy azonosítása, valamint nagyobb a jelszó illetéktelen kézbe kerülésének veszélye is. A Verizon Business Risk Team 2010-es elemzése szerint a biztonsági betörések, adatlopások csaknem felét cégen belülről követik el, és ehhez jelentős részben hozzájárulnak az adminisztrátorok és a dolgozók részére feleslegesen kiutalt emelt szintű jogosultságok. A probléma néhány szerver és kis számú privilegizált alkalmazott esetén szigorú munkarenddel és egyszerűbb eszközök (pl. „sudo”) használatával még kezelhető, nagyobb kiterjedésű hálózatoknál azonban a számítógépes rendszereken tárolt adatok fontossága és értéke, az esetleges leállások, adatszivárgások, előírászegeségek várhatóan magas kárösszege elkerülhetetlenné teszi egy a privilegizált hozzáféréseket kezelő rendszer bevezetését.

A NetIQ Privileged User Manager kifinomult keretrendszert biztosít

az emelt szintű jogosultságot igénylő feladatok elvégzéséhez és auditálásához. Nem szükséges többé az összes rendszeradminisztrátor, adatbázis-adminisztrátor, és szoftverfejlesztő számára teljes körű jogosultságot adni, illetve a rendszeradminisztrátori fiók (UNIX/Linux: „root”, Windows: „Adminisztrátor”) jelszavát a tudomásukra hozni. A felhasználóknak csak a saját névre szóló, nem privilegizált felhasználói fiókjuk jelszavát kell ismerniük, a rendszer pedig ezen fiókon belülről biztosítja számukra az emelt szintű jogosultságot igénylő parancsok végrehajtását – a munkájukhoz feltétlenül szükséges mértékben, így minimalizálja a biztonsági kockázatokat. Központosított menedzsment eszközei és naplózása segítségével megkönnyíti a veszélyt jelentő műveletek rövid időn belüli felismerését és elhárítását, részletes auditálást biztosító eszközeivel pedig alapot teremt az utólagos elemzéshez és a megfelelési követelmények teljesítéséhez.

A megoldás az alábbi három részből tevődik össze:

- kiadott parancsok elfogása, rögzítése, és valós idejű elemzése
- szabályok kezelése, jogosultságok kiosztása, riasztás
- naplózás és auditálás

NetIQ megoldások

- Biztonsági megoldások

Termékek

- Privileged User Manager

Fontosabb képességek

- Rendszeradminisztrátori jogosultságot igénylő parancsok vagy a teljes munkamenetek elfogása, rögzítése, automatikus, valós idejű elemzése, kockázati besorolása
- A rögzített munkamenetek videolejátszó-szerű visszajátzása
- A szabályok részletesen meghatározhatják, melyik felhasználó, honnan, mikor, hogyan, milyen parancsokat adhat ki
- Intuitív, grafikus szabály-meghatározó felület, szabályváltozás-kezelés, beépített tesztkörnyezet
- SSH, illetve RDP relay a távoli kapcsolatok felügyeletére és naplózására
- Moduláris felépítés, beépített terheléelosztás, skálázható, redundáns, leállás nélkül frissíthető
- Biztonságos kommunikáció, beépített adatbázis és naplózás, teljes, zárt rendszer, opcionális adatbázis-titkosítás

Fontosabb előnyök

- A rendszergazdák saját felhasználói azonosítójukat használva végezhetik el a feladataikat
- Szükségtelemné válik a root szintű hozzáférés kiadása
- A vezetők számára gyors, egyszerű módszert kínál a rendszergazdai aktivitás ellenőrzésére
- Minden rendszergazdai aktivitást naplóz
- Automatikusan generálódó színekkel támogatott kockázatelemzés
- Jelentések az iparági és a törvényi szabályozásoknak való megfelelés igazolására
- Gyorsan bevezethető és egyszerűen felügyelhető megoldás



"Nem szerencsés, ha túl sok ember tudja a root jelszót. Eddig a sudo segítségével szabtuk határt ennek, de a sudo sajnos nehezen felügyelhető és csak korlátozott auditálási lehetőségeket biztosít. A NetIQ Privileged User Manager lehetővé tette, hogy szigorúbban kezeljük a rendszeradminisztrátori hozzáférést, és biztosítsuk a kellően részletes auditálást, amire szükségünk van."

Russel Havens, Infrastruktúra-menedzsment Vezető Elemző, ACS Inc.

www.netiq.hu

Parancsok elfogása és elemzése

A Command Control Agent modul a felhasználó és az operációs rendszer közé ékelődik be (a „shell” helyére), és minden kiadott parancsot továbbít a központi jogosultságkezelő adatbázishoz, amely azok végrehajtását a beállított szabályok szerint engedélyezi vagy megtiltja. Az egyes parancsokat, vagy akár a teljes munkamenetet rögzíti és automatikusan elemzi, majd az eseményeket elhelyezi egy kockázati skálán.

Szabályok kezelése, jogosultságok kiosztása, riasztás

A parancsok végrehajtását az üzemeltető által központilag beállított szabályok határozzák meg, melyeket egy felhasználóbarát, intuitív grafikus felület segít kialakítani. A szabályok részletesen meghatározhatják, hogy ki mit tehet, melyik felhasználó, mikor, honnan, milyen módon, milyen műveletet hajthat végre. Amennyiben a szabályok alapján egy parancs végrehajtása megengedett, úgy az a távoli gépen a „root” felhasználó jogosultságaival kerül végrehajtásra. A rendszer képes naplózni az egyes billentyűleütéseket csak úgy, mint az egérkattintásokat, így utólag minden tevékenység visszajátszható egy videólejátszóhoz hasonló felületen. A rögzített munkamenet valós időben kockázatelemzésnek veti alá, képes rendkívül nagy mennyiségű naplóadatból is kiszűrni az értékes információkat, és a gyanúnak tűnő műveletekről riasztást ad ki.

Naplózás és auditálás

A Compliance Auditor különböző szűrők segítségével kiválasztja az auditorok számára érdekes eseményeket, melyeket színekkel jelöl meg a kockázati szint alapján. Az auditorok részére e-mail-ben értesítést küld, így a legveszélyesebb és leggyanúsabb parancsok rövid időn belül kiszűrhetők és megvizsgálhatók, amennyiben elfogadásra kerülnek, úgy elektronikus aláírással is elláthatók. Az elvárható gondosság („due diligence”) garantálásával teljesíthetők a PCI-DSS, SOX, és más előírások.

Architektúra és bevezetés

A Privileged User Manager egy moduláris felépítésű rendszer, amely lehetővé teszi, hogy az egyes feladatokat a megfelelő skálázódás érdekében több szerverre osszuk szét, illetve redundanciát biztosítsunk, ami kiküszöböli az egyponthiba lehetőségét, és biztosítja a rendszermodulok leállás nélkül történő frissítését. A moduláris felépítés miatt nem szükséges a teljes hálózati forgalmat keresztülvezetni egy központi rendszeren, ez javítja a skálázhatóságot és fájdalommentessé teszi a bevezetést. Integrált naplózórendszert és adatbáziskezelőt tartalmaz, így önállóan is megállja a helyét, de remekül integrálható a NetIQ Sentinel (SIEM) és a NetIQ Identity Manager (IDM) rendszerekkel egy teljes körű megfelelőség-kezelési megoldás érdekében. A központosított adminisztráció és szabálykezelés révén a frissítések és konfigurációs változtatások elvégzéséhez szükséges idő a versenytárs rendszerekhez képest akár a tizedére is csökkenhet.

Újdonságok a PUM 2.3 verzióban

Az új verzió legfőbb újdonsága a Windows támogatása (pl. Windows Server 2003 és 2008, 32/64-bit). A Windows támogatás nagyrészt ugyanazokat a képességeket nyújtja, mint a UNIX/Linux rendszerek esetében. Biztonságosan tárolja a Windows jelszavakat, melyeket az adminisztrátorok nem ismernek, a Command Control Agent-tel történő azonosítás során és a parancsvégrehajtási szabályok vizsgálatakor a Windows felhasználói- és csoportjogosultságokat is figyelembe veszi, sőt támogatja az Active Directory és más LDAP (pl. eDirectory) azonosítást is. Beléptetés után egy RDP csatornát hoz létre, ezen keresztül lehet az adminisztratív teendőket elvégezni, az itt történtek pedig ugyanúgy rögzítésre kerülnek, mint a UNIX/Linux esetében. További fontos újdonság az SSH Relay szolgáltatás, amely UNIX/Linux környezetben lehetővé teszi egy ügynökprogram nélküli architektúra kialakítását is.

Keresse meg helyi megoldásszállítóját, vagy vegye fel a kapcsolatot a NetIQ magyarországi képviselői irodájával az alábbi elérhetőségek valamelyikén:

MOM Park, SAS torony
1124 Budapest, Csörsz u. 45.
Tel: +36 (1) 489-4600
Fax: +36 (1) 489-4601
info@netiq.hu
www.netiq.hu

