

Novell Privileged User Manager

Zapewnienie kontroli dostępu do systemów Linux/UNIX

Novell.

Kontrola dostępu i audyt

Wiele przedsiębiorstw i instytucji zmagają się z poważnymi zagrożeniami, niepotrzebnie udostępniając dane uwierzytelniające do kont administracyjnych np. deweloperom czy administratorom IT od poszczególnych aplikacji i bazy danych. Oczywiście osoby te mogą potrzebować w swojej pracy uprzywilejowanego dostępu do systemów UNIX, Linux, Solaris czy AIX. Czy można mieć jednak pewność, że w trakcie korzystania przez nich z uprzywilejowanego dostępu systemy te są bezpieczne? Gdy dba o to Novell Privileged User Manager, odpowiedź brzmi: tak.

Novell Privileged User Manager (PUM) pomaga w zarządzaniu tożsamością i dostępem dla użytkowników uprzywilejowanych posiadających dostęp do kont typu **root**. Umożliwia on przydzielanie administratorom uprzywilejowanego dostępu, ale bez potrzeby logowania się na konto root. Działanie systemu opiera się na centralnej bazie danych osób i ich uprawnień, a końcowym efektem wdrożenia jest autoryzowany i w pełni kontrolowany (audyt!) dostęp do uprzywilejowanych komend i zarządzanie prawami administracyjnymi dla wszystkich użytkowników objętych kontrolą.

Novell Privileged User Manager wspierana następujące platformy:

- *IBM AIX 32-bit. i 64-bit., wersje 5.3 i 6.1*
- *HP-UX (PA-RISC) 32-bit. i 64-bit., wersje 11.11 i 11.23*
- *HP-UX (Itanium) 64-bit., wersja 11.23*
- *SUSE Linux Enterprise Server (SLES) 32-bit. i 64-bit., wersje 10 SP2 i 11*
- *Red Hat 32-bit i 64-bit., wersje 4.0 x86 i 5.0 x86*
- *IBM zSeries 64-bit z systemem SLES 10 SP2, SLES 11 i Red Hat w wersji 5*
- *Sun Solaris (SPARC) 32-bit. i 64-bit., wersje 8, 9 i 10*
- *Sun Solaris (Intel) 32-bit. i 64-bit., wersje 8, 9 i 10*
- *HP Tru64 UNIX 64-bit., wersje 5.1a i 5.1b*
- *VMware ESX Server 64-bit, wersje 3.0 i 3.5*
- *Xen Hypervisor, wersje 3.2 i 3.3*

Zalety stosowania rozwiązania Novell Privileged User Manager

Dzięki Novell Privileged User Manager administratorzy nie potrzebują pełnego dostępu do systemów IT, by wykonywać swoją pracę. Zalogowanie się przy pomocy ID użytkownika wystarczy, aby wydawać wcześniej ustalone, uprzywilejowane polecenia na podstawie ustalonych zasad i polityki bezpieczeństwa, zarówno w odniesieniu do określonej osoby, jak i grupy, do której należy dany użytkownik.

Podstawowe zalety i korzyści płynące z korzystania z oprogramowania Novell Privileged User Manager:

- *Delegowanie dostępu do kont użytkownika root zamiast współdzielenia danych uwierzytelniających użytkownika root ze wszystkimi administratorami.*
- *Ograniczenie ryzyka wykonania nieautoryzowanych transakcji i uzyskanie nieautoryzowanego dostępu do informacji.*

- Ograniczenie dostępu do określonych zadań administracyjnych na serwerach Linux i Unix wyłącznie do autoryzowanych użytkowników.
- Możliwość zatwierdzania przez dodatkowe osoby operacji realizowanych przez administratorów (np. wykonywanie określonych komend).
- Pełna kontrola i audyt aktywności uprzywilejowanych użytkowników z rejestrowaniem naciśnięcia każdego klawisza.
- Wizualny audyt aktywności użytkowników z możliwością przeglądania nagranych sesji użytkowników.
- Analiza ryzyka wykonanych przez użytkowników operacji poprzez wbudowany inteligentny mechanizm oceny ryzyka.

Komponenty rozwiązania Novell Privileged User Manager

Centralna konsola dostępna przez przeglądarkę pozwala na proste administrowanie systemem. W porównaniu z produktami konkurencji, Novell Privileged User Manager można szybko wdrożyć, a sam system zapewnia krótsze czasy odpowiedzi i logowania zdarzeń oraz pełne audytowanie aktywności uprzywilejowanego użytkownika.



Rysunek 1: Centralna konsola dostępna przez przeglądarkę

Poniżej omówiono poszczególne funkcje i narzędzia dostępne w konsoli oprogramowania Novell Privileged User Manager.

Compliance Auditor

Audyt zgodności z przepisami, regulacjami czy wewnętrznymi regułami zapewnia działające uprzedzająco narzędzie audytowe. Służy ono także do przeglądania logów i analizy zgodnie z predefiniowanymi rolami. Pozwala osobom audytującym na sprawdzenie wykonywanych operacji, odtworzenie pełnej aktywności uprzywilejowanego użytkownika oraz przygotowanie notatek na potrzeby audytu. Informacje do analizy i audytu pobierane są w zdefiniowanych przedziałach czasu – np. co godzinę, dzień, tydzień.

Framework User Manager

Zarządzanie uprzywilejowanymi użytkownikami, ich uprawnieniami oraz rolami w systemie odbywa się za pomocą intuicyjnego, graficzny interfejsu.

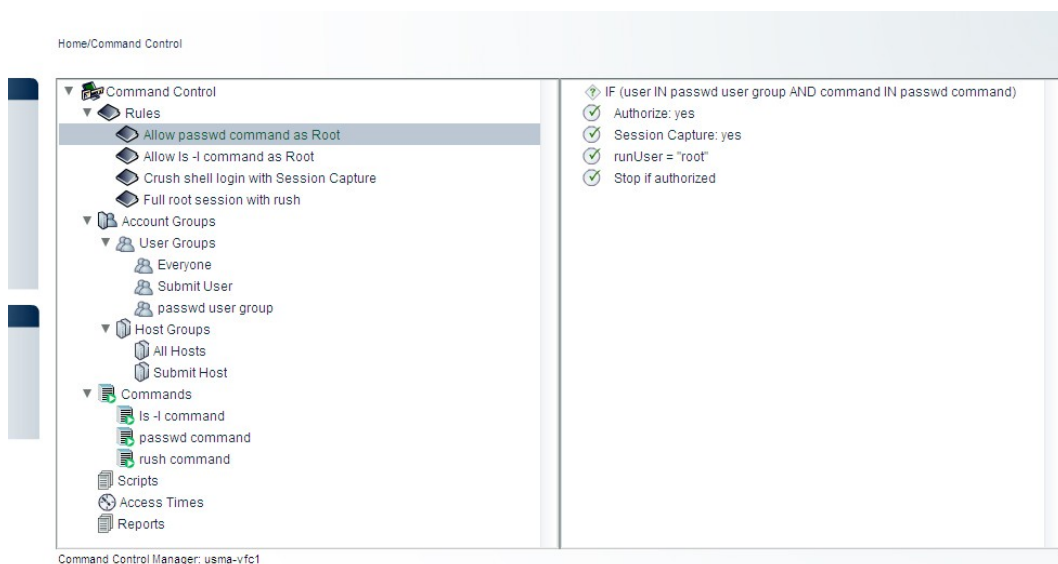
The screenshot shows the 'Modify User Group' configuration page. It includes the following fields and sections:

- Name:** A text input field containing 'passwd user group' and a 'Disabled' checkbox.
- Description:** A text area containing 'This user groups defines the user accounts that will be matched to allow the passwd command to be run as root'.
- Manager Name:** A text input field containing 'Jack Smith' and a dropdown menu.
- Manager Tel.:** An empty text input field.
- Manager Email:** An empty text input field.
- Users:** A list box containing 'tusr1', 'tusr2', 'YF4521', and 'P03873'.
- User Groups:** A list box containing 'Everyone' and 'Submit User', both with unchecked checkboxes.
- Buttons:** 'Sort', 'Finish >', and 'Cancel' buttons at the bottom.

Rysunek 2: Tworzenie grup użytkowników z określonym uprawnieniami

Command Control

Narzędzie do zarządzania wydawaniem komend przez uprzywilejowanych użytkowników zgodnie z przypisanymi im rolami w systemie.



Rysunek 3: Zarządzanie użytkownikami, ich uprawnieniami oraz rolami w systemie

Hosts

Privileged User Manager jest przygotowany do obsługi nawet bardzo rozbudowanego środowiska IT. Z poziomu funkcji *Hosts* można centralnie zarządzać instalacjami oprogramowania Privileged User Manager, aktualizacjami, wyrównaniem obciążenia (*load-balancing*), wysoką dostępnością zasobów i alertami.

Reporting

Funkcja raportowania zapewnia dostęp do przeszukiwarki informacji z logów oraz możliwość przeglądania logów w trybie podświetlenia ważnych informacji.

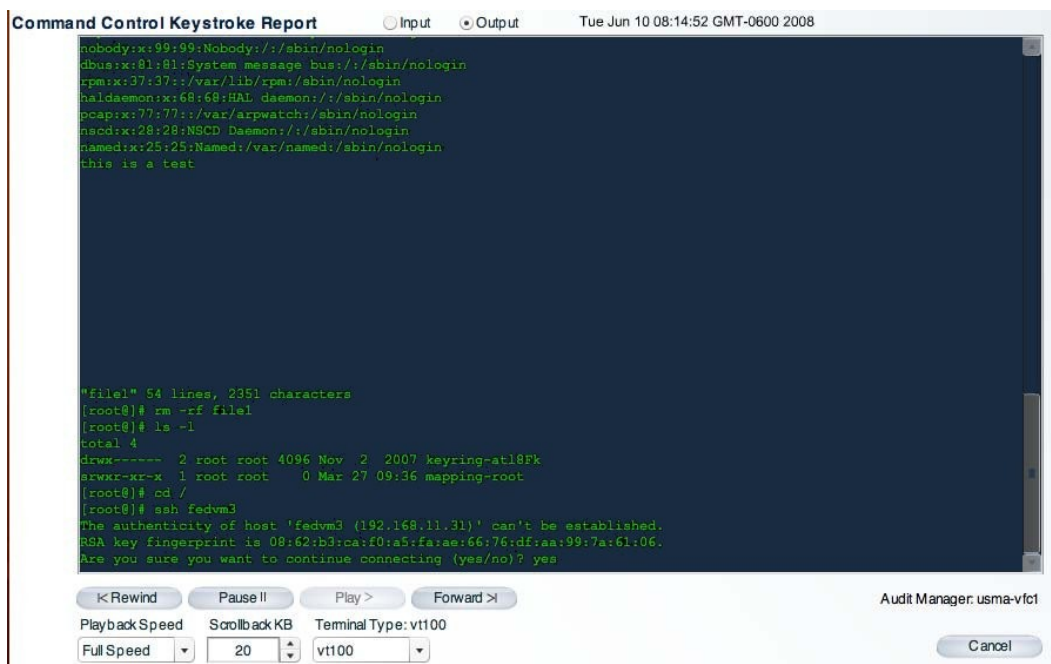
Package Manager

Narzędzie *Package Manager* pozwala w łatwy sposób aktualizować wszystkie komponenty oprogramowania Novell Privileged User Manager.

Korzyści płynące z korzystania z systemu Novell Privileged User Manager

Zarządzanie ryzykiem

Novell Privileged User Manager zarządza upoważnionym dostępem do systemów przez użytkowników uprzywilejowanych poprzez scentralizowany mechanizm polityk, pozwalający na konfigurację zasad kontrolujących aktywność użytkowników na podstawie tożsamości użytkownika, wpisanego przez niego polecenia, nazwy hosta oraz czasu. Taki sposób zarządzania przywilejami daje kontrolę nad tym, do jakich poleceń, w jakim czasie i z jakiego miejsca poszczególni użytkownicy uzyskują dostęp. Wszelkie działania użytkowników są rejestrowane, co pozwala na podjęcie interwencji w przypadku podejrzanej aktywności.



The screenshot displays a 'Command Control Keystroke Report' window. At the top, it shows 'Input' and 'Output' tabs, and a timestamp 'Tue Jun 10 08:14:52 GMT-0600 2008'. The main content is a terminal window with the following text:

```
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpm:x:37:37:/:/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
pcap:x:77:77:/:/var/arpwatch:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
this is a test

"file1" 54 lines, 2351 characters
[root@]# rm -rf file1
[root@]# ls -l
total 4
drwx----- 2 root root 4096 Nov  2 2007 keyring-atl8Fk
srwxr-xr-x  1 root root   0 Mar 27 09:36 mapping-root
[root@]# cd /
[root@]# ssh fedvm3
The authenticity of host 'fedvm3 (192.168.11.31)' can't be established.
RSA key fingerprint is 08:62:b3:ca:f0:a5:fa:ae:66:76:df:aa:99:7a:61:06.
Are you sure you want to continue connecting (yes/no)? yes
```

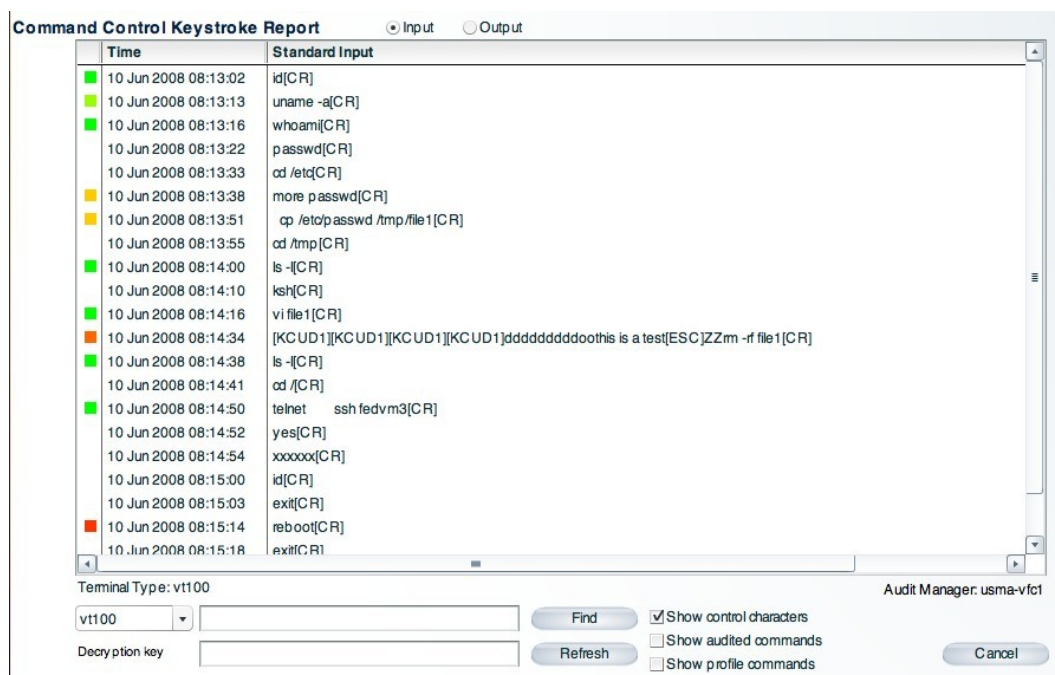
At the bottom of the window, there are playback controls: 'Rewind', 'Pause', 'Play', and 'Forward' buttons. Below these are 'Playback Speed' (set to 'Full Speed'), 'Scrollback KB' (set to '20'), and 'Terminal Type' (set to 'vt100'). A 'Cancel' button is located at the bottom right.

Rysunek 5: Działania użytkowników uprzywilejowanych są rejestrowane, co umożliwia ich późniejsze przeglądanie i analizę

Intuicyjny interfejs typu „przeciągnij i upuść” ułatwia tworzenie reguł i eliminuje konieczność skomplikowanego, ręcznego pisania skryptów. Ponadto, zintegrowane narzędzie do testów pozwala administratorom na przetestowanie nowych kombinacji reguł przed dopuszczeniem ich do wykorzystania w produkcji. Reguły można po prostu przeciągnąć do zagnieżdżonych hierarchicznie struktur, aby zbudować wyszukane instrukcje sterujące, których użycie w połączeniu ze skryptami może zapewnić bardziej drobiazgową kontrolę nawet dla najbardziej wymagających środowisk.

Rejestrowanie aktywności oparte na analizie ryzyka

Novell Privileged User Manager zawiera inteligentny mechanizm analizujący ryzyko, co pomaga zachować równowagę pomiędzy poziomem szczegółowości a ilością gromadzonych informacji. Mechanizm ten analizuje aktywność użytkownika i przypisuje jej poziom ryzyka od 0 do 9 na podstawie oceny rodzaju wydanego polecenia, tożsamości użytkownika, lokalizacji, z której to zrobił. Polecenia o wysokim poziomie ryzyka oznaczone są dodatkowo kolorem czerwonym, te o niskim poziomie – kolorem zielonym, a reszta poleceń oznaczona jest różnymi odcieniami tych kolorów, aby umożliwić natychmiastową identyfikację ryzykownych wydarzeń.



Rysunek 6: Centralna kontrola działań użytkowników uprzywilejowanych

Raportowanie oparte na informacji o ryzyku

Novell Privileged User Manager automatycznie filtruje dane, co pozwala kierownictwu na pozyskanie ustalonej ilości informacji z głównej bazy danych audytu – ze zdefiniowaną częstotliwością (raz na godzinę, raz dziennie, raz na tydzień lub raz na miesiąc). Osoby te mogą również wprowadzić dodatkowe kryteria filtrowania danych, np. w celu wyświetlenia tylko wydarzeń o wysokim poziomie ryzyka, które wystąpiły w określonym przedziale czasowym.

Zaawansowana analiza wykonywanych komend i operacji

Unikalna umiejętność profilowania oceny ryzyka oferowana przez rozwiązanie Novell Privileged User Manager umożliwia szybką i łatwą identyfikację danych o podwyższonym poziomie ryzyka, pozwalając na zmniejszenie potencjalnych zniszczeń spowodowanych złośliwą aktywnością czy też przypadkowym, niewłaściwym użytkowaniem. Każdą część zarejestrowanych sesji można podejrzeć i przeanalizować krok po kroku. Pomocny jest w tym intuicyjny interfejs i wszechstronne narzędzia do nawigacji. Ponadto, informacje o aktywności użytkowników można przeszukiwać i zaznaczać według wielu różnych kryteriów. Co więcej, istnieje możliwość zapisywania w logach każdego wciśnięcia klawisza przez uprzywilejowanego użytkownika.

Podsumowanie

Novell Privileged User Manager zarządza uprzywilejowanym dostępem administratorów stosując scentralizowany mechanizm polityk. Konfiguracja reguł dla działań użytkowników uprzywilejowanych odbywa się na podstawie wielu parametrów, jak tożsamość użytkownika, wpisane przez niego polecenie, czas i miejsce tego zdarzenia (w skrócie: kto, co, gdzie i kiedy). Taki sposób zarządzania przywilejami daje kontrolę nad tym, do jakich poleceń, w jakim czasie i z jakiego miejsca poszczególni użytkownicy mają dostęp. Wszelkie działania użytkowników uprzywilejowanych są rejestrowane, co pozwala na podjęcie interwencji w przypadku podejrzanej aktywności.

Novell Privileged User Manager obsługuje szeroką gamę systemów Linux i UNIX. Proponuje proste, aczkolwiek wysoce skuteczne rozwiązanie do obniżenia ryzyka i poprawy bezpieczeństwa w przedsiębiorstwie, co sprawia, że niewielkie koszty związane z inwestycją w Novell Privileged User Manager szybko się zwracają.

Więcej informacji o oprogramowaniu Novell Privileged User Manager można znaleźć na stronie:

www.novell.com/products/privilegedusermanager.

W celu uzyskania szczegółowych informacji o cenach i licencjonowaniu prosimy kontakt:

Novell Sp. z o.o.

ul. Postępu 21

02-676 Warszawa

tel. 0 22 537 5000

bezpłatna infolinia 0 800 22 66 85

infolinia@novell.pl