nVision 10

Podstawowym bytem w programie Axence nVision 9 była ikona urządzenia – to ona grupowała zarówno dane z monitorowania sieciowego, inwentaryzację jak i również aktywność użytkowników, którzy pracowali na danej stacji roboczej. Takie podejście dobrze sprawdzało się kilka lat temu, gdzie można było przyjąć, że na jednym komputerze pracuje jeden użytkownik. Niemniej, wraz z dynamicznym rozwojem infrastruktury wykorzystywanej w wielu przedsiębiorstwach także w Axence nVision, w zaawansowanym programie do monitorowania i zarządzania siecią komputerową, podejście to zostało zweryfikowane i dostosowane do wymagań rynku.
W najnowszej, 10. wersji programu, kontekst urządzenia wzbogacony został o nowy byt w programie - kontekst użytkownika. W nowej wersji programu dane, które w sposób niepodważalny dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych, zostały odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie.
Wierzymy, że funkcje te ułatwią gromadzenie, edycję a przede wszystkim prezentowanie informacji dotyczących konkretnego pracownika oraz przyznawanie dostępów.

A. Model ustawień monitorowania i blokowania.

1. Ustawienia monitorowania i blokowania

W odróżnieniu do nVision 9 (w której ustawienia były zachowane w postaci zestawu reguł, czyli w profilach Agentów) najnowsza wersja Axence nVision 10, ustawienia monitorowania użytkowników i blokowania stron oraz aplikacji, konfiguruje na grupach użytkowników.
To w ich właściwościach administrator powinien skonfigurować opcje monitorowania, ponieważ konta użytkowników dziedziczą z nich ustawienia. Oczywiście konto każdego z użytkowników może przynależeć do więcej niż jednej grupy – wtedy efektywne ustawienia monitorowania będą stosowane zgodnie z zasadami opisanymi poniżej.
Podstawowymi nośnikami ustawień monitorowania w najnowszej wersji programu są: Atlas, Grupy użytkowników, konto użytkownika.

a. Atlas – ustawienia domyślne

Atlas jest podstawowym obiektem w nVision 10, który zawiera podstawowe, globalne ustawienia monitorowania. Oznacza to, że konto każdego użytkownika, który nie należy do żadnej z grup, przyjmie ustawienia monitorowania, które przypisane są do Atlasu.

Możliwe konfiguracje:

- Monitorowanie

Ustawienie	Możliwe wartości	Uwagi
Użycie łącza	**monitoruj** / nie monitoruj	domyślnie: monitoruj
Odwiedzone strony WWW	**monitoruj** / nie monitoruj	domyślnie: monitoruj
Użycie aplikacji	**monitoruj** / nie monitoruj	domyślnie: monitoruj
Czas pracy	**monitoruj** / nie monitoruj	domyślnie: monitoruj
Wydruki	**monitoruj** / nie monitoruj	domyślnie: monitoruj
E-maile	monitoruj / **nie monitoruj**	domyślnie: nie monitoruj

Ustawienie	Możliwe wartości	Uwagi
Przesyłaj aktywność w czasie	monitoruj / **nie monitoruj**	domyślnie: nie monitoruj
Przerwy w aktywności	**monitoruj** / nie monitoruj	domyślnie: monitoruj
Zapisuj przerwy powyżej "X" minut	(liczba minut)	domyślnie: 5 minut
Czas monitorowania	Kiedykolwiek, pomiędzy, z wyjątkiem (godziny, dni tygodnia)	domyślnie: kiedykolwiek

Zdalny dostęp

Ustawienie	Możliwe wartości	Uwagi
Zezwól na podgląd pulpitu	**zezwól** / nie zezwalaj	domyślnie: zezwól
Zezwól na zdalny dostęp	**zezwól** / nie zezwalaj	domyślnie: zezwól
Pokaż powiadomienie	**nie powiadamiaj** / powiadamiaj	domyślnie: nie powiadamiaj
Pytaj o zgodę użytkownika	nie pytaj / **zapytaj**	domyślnie: zapytaj
Zezwól, jeżeli użytkownik nie odpowiada	**zezwól** / nie zezwalaj	domyślnie: zezwól

Wyświetlanie Agenta

Ustawienie	Możliwe wartości	Uwagi
Pokaż ikonę Agenta	**pokaż** / nie pokazuj	domyślnie: pokaż
Po zalogowaniu pokaż informację o Agencie	**pokaż** / nie pokazuj	domyślnie: pokaż
Pokaż informację o monitorowaniu aktywności użytkownika	**pokaż** / nie pokazuj	domyślnie: pokaż

Domyślnie Atlas zawiera taki zestaw ustawień monitorowania, aby każdy nowy użytkownik objęty był maksymalnie restrykcyjnym monitorowaniem.

b. Grupy użytkowników

Grupy użytkowników mogą zawierać dowolną liczbę kont użytkowników oraz podgrup. Jeżeli grupa użytkowników nie jest podgrupą, wtedy jej obiektem nadrzędnym, z którego dziedziczy ustawienia, jest Atlas.

W konfiguracji ustawień grupy (lub podgrupy) można definiować jedynie ustawienia, które są wyjątkami mniej restrykcyjnymi od ustawień nadrzędnych (Atlasu lub grupy, która zawiera daną podgrupę). Np. na poziomie Atlasu włączono monitorowanie wydruków – zatem na poziomie grupy możliwe jest jedynie wyłączenie monitorowania wydruków.

Takie podejście pozwala na wyłączenie pewnej grupy użytkowników z monitorowania.

Możliwe konfiguracje wyjątków na poziomie grupy:

Monitorowanie

Ustawienie	Możliwe wartości
Użycie łącza	nie monitoruj
Odwiedzone strony WWW	nie monitoruj
Użycie aplikacji	nie monitoruj
Czas pracy	nie monitoruj
Wydruki	nie monitoruj
E-maile	nie monitoruj
Przesyłaj aktywność w czasie	nie monitoruj
Przerwy w aktywności	nie monitoruj
Czas monitorowania	Czas monitorowania można ustawić tylko w Atlasie lub indywidualnie dla każdego użytkownika.

Zdalny dostęp

Ustawienie	Możliwe wartości
Zezwól na podgląd pulpitu	nie pozwalaj
Zezwól na zdalny dostęp	nie pozwalaj
Pokaż powiadomienie	powiadom
Pytaj o zgodę użytkownika	zapytaj
Zezwól, jeżeli użytkownik nie odpowiada	nie pozwalaj

Wyświetlanie Agenta

Ustawienie	Możliwe wartości
Pokaż ikonę Agenta	nie pokazuj
Po zalogowaniu pokaż informację o Agencie	nie pokazuj
Pokaż informację o monitorowaniu aktywności użytkownika	nie pokazuj

Domyślnie, żadna grupa nie zawiera żadnych wyjątków od ustawień nadrzędnych (Atlasu).

Wyjątki zdefiniowane dla grupy propagowane są również na jej wszystkie podgrupy. Nie można w żaden sposób „wyłączyć" grupy z propagowania ustawień lub wyjątków z bytów nadrzędnych.
Wyjątki zdefiniowane dla grupy wpływają na ustawienia wszystkich użytkowników, którzy do niej należą (z wyjątkiem tych, którzy mają zdefiniowane indywidualne ustawienia). Jeżeli użytkownik znajduje się w więcej niż jednej grupie, to aplikują się do niego wszystkie wyjątki ze wszystkich tych grup.

c. Użytkownik

Konto użytkownika może podlegać ustawieniom monitorowania, które są wynikiem ustawień Atlasu i grup lub może korzystać z indywidualnych ustawień monitorowania.

Ustawienia indywidualne umożliwiają konfigurację indywidualnych ustawień monitorowania, które będą miały zastosowanie tylko i wyłącznie dla konta użytkownika, dla które zostały ustawione, niezależnie od ustawień globalnych i wyjątków grup.

Ustawienia wynikowe to ustawienia globalne Atlasu po uwzględnieniu wyjątków ze wszystkich grup, do których należy dane konto użytkownika. Jeśli konto użytkownika przynależy do kilku grup, dla których skonfigurowano różne ustawienia tego samego parametru monitorowania, to wynikowo zastosowane będzie ustawienie mniej restrykcyjne (np. nie monitoruj użycia aplikacji).

Dla każdego z ustawień, administrator może wybrać zastosowanie ustawienia wynikowego lub indywidualnego (np. wynikowym będzie ustawienie czasu pracy a indywidualnie przydzielonym ustawienie użycia aplikacji).

d. Podsumowanie

Wprowadzenie nowego modelu ustawień monitorowania pozwala na zastosowanie intuicyjnego sposobu sumowania ustawień, który wynika z faktu przynależenia konta danego użytkownika do wielu grup (konto będzie objęte wszystkimi wyjątkami, wszystkich grup, do których należy).
Zupełnie nowe podejście do zarządzania ustawieniami monitorowania określa, że ustawienia grupy nie mogą być użyte do zwiększenia uprawnień a jedynie do ich ograniczenia. Pozwala to na zastosowanie dobrej praktyki korzystania z Axence nVision 10 – budowania przejrzystych reguł monitorowania sieci.
Przykład: globalne włączenie monitorowania czasu pracy i użycia aplikacji a następnie wyłączanie tego ustawienia w drodze wyjątków na poziomie grup użytkowników

2. Ustawienia Blokowania Stron, Aplikacji, Pobierania Plików

Podstawowymi nośnikami ustawień blokowania w najnowszej wersji programu są: Atlas, Grupy użytkowników, konto użytkownika.
W przeciwieństwie do ustawień monitorowania (które mają z góry zdefiniowaną listę możliwych ustawień), ustawienia blokowania opierają się na definiowaniu dowolnie dużej liczby reguł blokowania.
Atlas nie zawiera żadnych domyślnych ustawień blokowania o ile nie zostały one utworzone w wyniku procesu migracji danych z nVision 9.

a. Ustawienia blokowania

Blokowanie stron

W nVision 10 usunięta została domyślna akcja blokowania stron: „Zablokuj wszystkie strony oprócz poniższych". W sytuacji, gdy administrator nie skonfigurował żadnych reguł blokad stron, dostęp do wszystkich stron internetowych nadal jest możliwy (program zachowuje się tak, jakby akcja domyślna była zawsze ustawiona na „zezwól na wszystkie strony oprócz poniższych"). W praktyce oznacza to, że każda strona, która nie pasuje do żadnej ze zdefiniowanych reguł, nie jest blokowana.

W programie można zdefiniować dowolnie dużą liczbę reguł blokowania stron.
Każda reguła zawiera swoją nazwę, rodzaj akcji, domenę (lub adres IP) i efektywny czas obowiązywania.

- Akcja reguły to jedna z dwóch opcji: „zezwól" lub „blokuj".
- Domena (lub adres IP) to wzorzec, do którego dopasowywane będą odwiedzane strony.
  We wzorcu można używać znaku „*", który oznacza dopasowanie dowolnego ciągu znaków.
- Efektywny czas obowiązywania to wzorzec czasowy w który można wyszczególnić dni tygodnia lub godziny w obrębie dnia.
  Jeżeli czas obowiązywania został zdefiniowany, to poza tym czasem reguła jest ignorowana.

Jeżeli odwiedzona strona pasuje do więcej niż jednej reguły, to:

- Jeżeli wszystkie z tych reguł mają akcję „blokuj", to strona jest blokowana.
- Jeżeli co najmniej jedna z tych reguł ma akcję „zezwól", to strona nie jest blokowana.

Jeżeli odwiedzona strona nie pasuje do żadnej reguły, to również nie jest blokowana.

Blokowanie aplikacji
Analogicznie jak dla blokowania stron, w programie zdefiniować można dowolnie dużą liczbę reguł blokowania aplikacji.

Każda reguła zawiera swoją nazwę, nazwę blokowanego pliku wykonywalnego i efektywny czas obowiązywania.

- Dla reguł blokowania aplikacji nie można zdefiniować akcji „zezwól" (każda z tych reguł jest zawsze z akcją „blokuj").
- We wzorcu nazwy blokowanego pliku wykonywalnego również można używać znaku „*".

Jeżeli uruchomiona aplikacja nie pasuje do żadnej reguły, to nie jest blokowana.

Blokowanie rozszerzeń pobieranych plików
Analogicznie jak dla blokowania stron, w programie zdefiniować można dowolnie dużą liczbę reguł blokowania rozszerzeń pobieranych plików.

Każda reguła zawiera swoją nazwę i zablokowane rozszerzenie pliku.

- Dla reguł blokowania rozszerzeń pobieranych plików nie można zdefiniować akcji „zezwól" (każda z tych reguł jest zawsze z akcją „blokuj").
- We wzorcu zablokowanego rozszerzenia pliku nie można używać znaku „*".
- Reguły blokowania rozszerzeń pobieranych plików nie mają efektywnego czasu obowiązywania (obowiązują cały czas).

Jeżeli rozszerzenie ściągniętego pliku nie pasuje do żadnej reguły, to nie jest blokowane.

b. Dziedziczenie ustawień blokowania

Atlas
Atlas jest podstawowym obiektem w nVision 10, który zawiera podstawowe, globalne ustawienia blokowania. Oznacza to, że konto każdego użytkownika, który nie należy do żadnej z grup, przyjmie ustawienia monitorowania, które przypisane są do Atlasu.
Atlas nie dziedziczy ustawień z żadnego innego bytu.
Atlas nie zawiera żadnych domyślnych ustawień blokowania o ile nie zostały one utworzone w wyniku procesu migracji danych z nVision 9.

Grupy użytkowników
Każda grupa użytkowników zawiera wszystkie reguły blokowania Atlasu oraz grup nadrzędnych, do których należy.
Na poziomie grupy nie można w żaden sposób modyfikować reguł odziedziczonych z Atlasu ani z grup nadrzędnych. Nie można ich również usuwać ani wyłączać z dziedziczenia.
Na poziomie grupy można zdefiniować dowolnie dużą liczbę reguł indywidualnych, które zostaną dołączone do zbioru tych odziedziczonych.
Reguły indywidualne zdefiniowane w grupie są dziedziczone przez wszystkie grupy podrzędne, które do niej należą.

Użytkownik
Konto użytkownika korzysta z reguł odziedziczonych z grup (i Atlasu) oraz z reguł indywidualnych.
Dla pojedynczego użytkownika można wyłączyć dziedziczenie reguł blokowania z Atlasu i grup.

- Jeżeli użytkownik ma włączone dziedziczenie reguł, to obowiązuje go sumaryczna kolekcja:reguł odziedziczonych z atlasu (jeżeli nie jest w żadnej grupie),
- reguł odziedziczonych ze wszystkich grup, w których się znajduje,
- reguł indywidualnych zdefiniowanych na poziomie tego użytkownika.

Jeśli konto użytkownika przynależy do kilku grup, dla których skonfigurowano różne reguły blokowania, to wynikowo zastosowane będą reguły blokowania.

Jeżeli użytkownik ma wyłączone dziedziczenie reguł, to obowiązują go wyłącznie jego reguły indywidualne.

c. Podsumowanie

- Jeżeli zablokowano jakąś stronę globalnie, to można określić grupę użytkowników, którzy będą mieć do niej dostęp.
- Jeżeli nie zablokowano jakiejś strony globalnie, to można określić grupę użytkowników, dla których będzie zablokowana.
- Jeżeli użytkownik znajduje się w grupie, która posiada regułę „zezwól" dla jakiejś strony, to nie można jej nadpisać regułą „blokuj" dołączając go do innej grupy.
- Funkcję „białej listy" („zablokuj wszystkie strony oprócz poniższych") można nadal zrealizować za pomocą reguły „blokuj" dla domeny „*".
- Jeżeli zablokowano globalnie jakąś aplikację lub rozszerzenie pobieranego pliku, to nie można ich odblokować na poziomie grupy.
- Jeżeli nie zablokowano globalnie jakiejś aplikacji lub rozszerzenia pobranego pliku, to można określić grupę użytkowników, dla których te byty będą zablokowane.
- Na poziomie użytkownika można zawsze można zdefiniować indywidualny zestaw reguł, niezależnie od sposobu działania mechanizmu dziedziczenia.

B. Migracja danych z nVision 10

1. Konta użytkowników

W wyniku migracji danych z nVision 9, do kont użytkowników synchronizowanych z Active Directory zostanie przepisana aktywność z ikon urządzeń ze starszej wersji programu.

Dla każdego konta lokalnego z Agenta nVision 9, na którym ktoś przynajmniej raz się zalogował, utworzone zostanie konto użytkownika w nVision 10.

2. Ustawienia monitorowania

a. Ustawienia monitorowania

Ustawienia monitorowania dostępne w nVision 9 w profilach Agentów, w nowej wersji nVision 10 przeniesione zostały na użytkowników i grupy.

Ustawienia domyślne

Ustawienia domyślne to ustawienia zmigrowane z nVision 9 i przypisane do Atlasu.
Wyznaczenie domyślnych ustawień monitorowania w nVision 10, sprowadza się do zsumowania wszystkich ustawień zawartych w profilu Agentów z nVision 9, z których korzystało przynajmniej 1 konto użytkownika, przy czym:

- jeżeli wybrana opcja była monitorowana w przynajmniej jednym profilu Agenta w nVision 9, w wyniku migracji danych do nVision 10, jest ona monitorowana w domyślnych ustawieniach,
- jeżeli aktywność w czasie była przesyłana w przynajmniej jednym profilu, to w wyniku migracji jest ona przesyłana w domyślnych ustawieniach,
- jeżeli przerwy w aktywności były wykrywane przynajmniej w jednym profilu, to w wyniku migracji są również wykrywane,
- zmigrowany czas przerwy w domyślnych ustawieniach to minimalny czas wybrany ze wszystkich dotychczasowych profili Agentów,
- zakres czasowy monitorowania w domyślnych ustawieniach to suma wszystkich zakresów występujących w dotychczasowych profilach Agentów:
  - jeżeli zakresy czasowe nie zachodzą na siebie, przy migracji danych wyznaczany jest nowy zakres, za początek którego przyjmowana jest najwcześniejsza a za koniec: najpóźniejsza godzina ze wszystkich dotychczasowych profili (np. zakresy 8:00 – 12:00 oraz 15:00 – 18:00 zostaną zmigrowane na zakres 8:00 – 18:00)
  - przypadek szczególny: jeśli przynajmniej jeden z profili miał ustawiony ciągły czas monitorowania, w wyniku migracji ustawieniem domyślnym będzie również monitorowanie ciągłe,
- jeżeli którykolwiek profil w nVision 9 zezwalał na podgląd pulpitu, dostęp zdalny lub pomijanie zgody użytkownika na zdalny dostęp, w zmigrowanych ustawieniach domyślnych również będą one dozwolone,
- jeżeli którykolwiek profil w nVision 9 zezwalał na wyświetlanie ikony Agenta, w domyślnych ustawieniach również będzie to dozwolone.

Ustawienia grup

W procesie migracji tworzone są grupy użytkowników, które są nośnikiem ustawień monitorowania wynikających z dotychczasowych profili Agentów. Każda grupa zawiera takie ustawienia monitorowania, aby użytkownik, który w niej się znajduje, objęty był takimi ustawieniami monitorowania jak w profilu Agenta w nVision 9.
Podczas migracji danych, tworzona jest nadrzędna grupa „Monitorowanie", która zawiera 3 podgrupy wbudowane:

- Grupy z profili,
- Grupy z map,
- Grupy z urządzeń.

Zarówno grupa nadrzędna jak i podgrupy wbudowane nie zawierają żadnych ustawień wbudowanych.

W podgrupach wbudowanych zostaną utworzone grupy użytkowników, które przyjmą nazwy:

- profili monitorowania wykorzystywanych w nVision 9,
- map jeśli w nVision 9 korzystały one z indywidualnych ustawień,
- urządzeń, jeśli korzystały one z indywidualnych ustawień (czyli nie korzystały ani z profilu Agenta, ani z ustawień mapy).

Następnie do grup dopisane zostaną konta użytkowników, którzy pracowali na urządzeniach w określonych profilach w nVision 9.

Informacje dodatkowe:

- Nie jest migrowany zakres czasowy monitoringu na poziomie profilu (grupy). W wersji 10 programu nie można ustalać tych zakresów na poziomie grupy. Wszystkie zakresy czasowe ze wszystkich profili są zsumowane wyłącznie do jednego, globalnego zakresu w ustawieniach.
- Żaden z użytkowników nie otrzymuje w procesie migracji ustawień indywidualnych.
- W wyniku migracji, mogą zostać zwiększone efektywne uprawnienia użytkownika pracującego na więcej niż jednym komputerze. Przykładowo, jeżeli w nVision 9 użytkownik pracował na komputerze, na którym monitorowanie było włączone i na drugim, gdzie monitorowanie było wyłączone, użytkownik po migracji nie będzie monitorowany na obu komputerach (ponieważ wyjątek „nie monitoruj" będzie go obowiązywał na obu komputerach).
- Ustawienia monitorowania i blokowania w nVision były związane z ikoną urządzenia i mapą, na której się ono znajdowało. Stąd możliwe było definiowanie różnych polityk bezpieczeństwa dla nowych użytkowników (zależnie od lokalizacji komputera). W nVision 10 jest jeden zestaw domyślnych uprawnień dla każdego nowego użytkownika, zatem administrator musi ręcznie utworzyć grupy z uprawnieniami i każdorazowo przydzielać do nich nowych użytkowników.

b. Ustawienia blokowania stron

Ustawienia domyślne
Ustawienia domyślne to ustawienia zmigrowane z nVision 9 i przypisane do Atlasu.
Wyznaczenie domyślnych ustawień blokowania stron w nVision 10, sprowadza się do zsumowania wszystkich reguł typu „blokuj" zawartych w profilu Agentów z nVision 9. W ten sposób powstaje domyślny zestaw, który zawiera wszystkie reguły blokowania stron.

Ustawienia grup
W procesie migracji tworzone są grupy użytkowników, które są nośnikiem ustawień blokowania stron.
Podczas migracji danych, tworzona jest nadrzędna grupa „Filtrowanie", która zawiera 3 podgrupy wbudowane:

- Grupy z profili,
- Grupy z map,
- Grupy z urządzeń.

Zarówno grupa nadrzędna jak i podgrupy wbudowane nie zawierają żadnych ustawień wbudowanych.

W podgrupach wbudowanych zostaną utworzone grupy użytkowników, które przyjmą nazwy:

- profili monitorowania wykorzystywanych w nVision 9,
- map jeśli w nVision 9 korzystały one z indywidualnych ustawień,
- urządzeń, jeśli korzystały one z indywidualnych ustawień (czyli nie korzystały ani z profilu Agenta, ani z ustawień mapy).

Następnie do grup dopisane zostaną konta użytkowników, którzy pracowali na urządzeniach w określonych profilach w nVision 9.

Sposób przeniesienia ustawień:

- Dla Atlasu, każdej z sieci oraz Agentów, które korzystały z indywidualnych reguł blokowania stron, tworzone są grupy ustawień blokowania, które umieszczane są grupie nadrzędnej „Filtrowanie". Do grup przypisywani są użytkownicy (analogicznie do przeniesienia ustawień monitorowania).
- Każda grupa ustawień blokowania stron zawiera wszystkie reguły filtrowania, które dotychczas były przypisane do profilu. Reguły te są ustawiane jako indywidualne dla każdej z grup.

- Dla każdej reguły typu „blokuj” z ustawień domyślnych, która nie koliduje z żadną indywidualną regułą grupy, tworzona jest przeciwna reguła typu „zezwól” a następnie jest przypisywana jako reguła indywidualna grupy. W wyniku tego działania, odblokowywane są strony, które dotychczas nie były blokowane a w wyniku migracji ustawień mogły zostać zablokowane.
- Po przeniesieniu ustawień wykonywane jest usuwanie reguł nadmiarowych w ustawieniach domyślnych: usuwane są reguły „blokuj”, które zawierają się w innych regułach (np. reguła dla domeny „*.pl” zawiera regułę dla strony „domena.pl”).

Informacje dodatkowe:

- W ramach procesu migracji żaden z użytkowników nie otrzymuje indywidualnych reguł filtrowania stron.
- W wyniku migracji, użytkownik, który pracował na więcej niż jednym komputerze, może mieć mniej stron zablokowanych.
- Jeżeli ustawienia globalne blokują domenę „*” a indywidualne ustawienia grupy blokują tylko domenę „domena.pl”, to na poziomie grupy nie zostanie utworzona reguła „zezwól” dla domeny „*.”, ponieważ spowodowałoby to bezskuteczność reguły blokowania domeny „domena.pl”. Z tego powodu, po migracji część grup może potencjalnie blokować więcej stron niż analogiczne dla nich profile w wersji 9 programu.

c. Ustawienia blokowania aplikacji, rozszerzeń pobieranych plików i portów

Blokowanie aplikacji
Domyślne ustawienia blokowania aplikacji tworzone są poprzez zsumowanie wszystkich dotychczasowych reguł blokowania ze wszystkich profili (analogicznie do domyślnych reguł blokowania stron).
Podczas migracji danych, tworzona jest nadrzędna grupa „Blokowanie”, która zawiera 3 podgrupy wbudowane:

- Grupy z profili,
- Grupy z map,
- Grupy z urządzeń.

Zarówno grupa nadrzędna jak i podgrupy wbudowane nie zawierają żadnych ustawień wbudowanych.

W podgrupach wbudowanych zostaną utworzone grupy użytkowników, które przyjmą nazwy:

- profili monitorowania wykorzystywanych w nVision 9,
- map jeśli w nVision 9 korzystały one z indywidualnych ustawień,
- urządzeń, jeśli korzystały one z indywidualnych ustawień (czyli nie korzystały ani z profilu Agenta, ani z ustawień mapy).

Następnie do grup dopisane zostaną konta użytkowników, którzy pracowali na urządzeniach w określonych profilach w nVision 9.

Ustawienia te jednak zawsze będą bezskuteczne, ponieważ ustawienia domyślne zawsze będą tak samo lub bardziej restrykcyjne. Celem tej migracji jest wyłącznie umożliwienie zapoznania się z tym, co te profile zawierały wcześniej.

Blokowanie rozszerzeń pobieranych plików
Domyślne ustawienia blokowania rozszerzeń pobieranych plików tworzone są poprzez zsumowanie wszystkich dotychczasowych reguł ze wszystkich profili (analogicznie do domyślnych reguł blokowania stron).
Podobnie jak przy procesie migrowania reguł blokowania aplikacji, ustawienia z profili są przenoszone do odpowiadających im podgrup, które zostały wcześniej utworzone w nadrzędnej grupie „Filtrowanie”. Ustawienia te są również bezskuteczne i zostają zachowane tylko w celach informacyjnych.

Informacje dodatkowe:

- Ustawienia blokowania portów nie podlegają migracji, na użytkownika, ponieważ w nVision 10 powiązane są ustawieniami urządzenia.
- Ustawienia ze wszystkich profili blokowania aplikacji i blokowania rozszerzeń pobieranych plików są scalone do jednego bytu ustawień domyślnych i po migracji obowiązują wszystkich użytkowników. Jeżeli korzystałeś z różnych profili na wielu urządzeniach, wymagana będzie ręczna korekta konfiguracji programu po procesie migracji.

d. Powiadomienia o blokadach

W nVision 10, dla każdego z poniższych 4 typów powiadomień o blokowaniu, można skonfigurować dokładnie jedną wersję:

- powiadomienia o zablokowaniu strony,
- powiadomienia o zablokowaniu aplikacji,
- powiadomienia o zablokowaniu pliku,
- powiadomienia o blokadzie portów.

W związku z tym, podczas procesu migracji sprawdzona zostanie liczba unikalnych powiadomień o blokadach z wersji 9 a do nowej wersji systemu zostanie przepisane to powiadomienie, które występuje najliczniej (dla każdego z 4 typów powiadomień).

e. Zrzuty ekranowe

Zrzuty ekranowe wykonane w wersji 9 programu na poziomie urządzenia, zostaną przeniesione do użytkownika, w kontekście którego zostały wykonane.
Ustawienie zbierania zrzutów ekranowych na poziomie urządzenia nie jest migrowane. Po procesie migracji należy ręcznie włączyć to ustawienie na poziomie każdego użytkownika, dla którego zrzuty mają być zapisywane. Z założenia, mechanizm zrzutów ekranowych jest tymczasowy i włączany okresowo, stąd jego ustawienia nie są migrowane.

f. Ustawienia DataGuard

Prawa domyślne

W wyniku migracji ustawień z nVision 9 tworzony jest zbiór praw domyślnych poprzez zsumowanie praw przydzielonych dotychczas do Agentów oraz nadrzędnego bytu Active Directory (najwyższego poziomu „Zaufanych jednostek AD") w taki sposób, aby zawierał on maksymalnie restrykcyjny zbiór uprawnień. W wyniku sumowania bardziej restrykcyjnymi są:

- blokowanie nośnika,
- włączenie audytu operacji na plikach na nośniku.

Ustalenie maksymalnie restrykcyjnego zbioru uprawnień jako „Prawa domyślne" jest niezbędne, aby bezpośrednio po migracji zapewnić ciągłość ochrony danych przed wyciekiem dla każdego nowego użytkownika.

Przeniesienie ustawień DataGuard:

- Utworzona zostanie nadrzędna grupa „Reguły DataGuard", która nie zawiera zdefiniowanych żadnych własnych ustawień.
- Prawa DataGuard przypisane do Atlasu w nVision 9 porównywane są z domyślnymi prawami nVision 10.

  Następnie jako podgrupa nadrzędnej grupy „Reguły DataGuard" tworzona jest grupa „Grupa z Atlasu", do której przypisywane są wszystkie prawa różniące się od praw domyślnych. Do tej grupy przypisywane są prawa o wartościach takich, jakie poprzednio miał Atlas. Przypisane prawa są prawami indywidualnymi tej grupy.
- Dla każdej mapy tworzona jest grupa o nazwie „Grupa z mapy X", która jest podgrupą grupy Atlasu lub mapy nadrzędnej wynikającej z poprzedniej wersji programu. Do tej grupy, jako prawa indywidualne, przypisywane są wszystkie prawa różniące się od praw grupy mapy nadrzędnej lub Atlasu.
- Dla każdego Agenta, który korzystał z indywidualnych praw DataGuard tworzona jest „Grupa z urządzenia X", do której przypisywani są użytkownicy pracujący na tym Agencie w nVision 9.
- Konto każdego użytkownika niedomenowego umieszczana jest w grupach, które odpowiadają Agentom, na których pracował. Jeżeli użytkownik pracował na więcej niż jednym komputerze, zostanie przypisany do wszystkich grup, które odpowiadają Agentom, na których pracował.

Rezultatem migracji jest odwzorowanie uprawnień wynikających ze struktury Atlasu, map i Agentów z nVision 9 za pomocą maksymalnie uproszczonego schematu grup użytkowników. W ostatecznej strukturze nVision 10 znajdują się tylko grupy, które w jakiś sposób zmieniają uprawnienia. Prawa DataGuard użytkowników domenowych nie ulegają zmianie.

Informacje dodatkowe:

- Po migracji do nVision 10 na każdego nowego użytkownika mogą zostać nałożone większe ograniczenia, nawet jeżeli zostanie utworzony na Agencie, który poprzednio nie miał żadnych blokad w module DataGuard.
- Ponieważ usunięty zostaje nadrzędny byt „Active Directory", który agregował uprawnienia dla wszystkich użytkowników z AD, utracone zostaną ustawienia które zostały w nim zdefiniowane. Pozostałe uprawnienia grup i użytkowników z Active Directory nie są w żaden sposób modyfikowane w trakcie procesu migracji.
- W wyniku migracji może się okazać, że na użytkowników z Active Directory zostaną nałożone większe ograniczenia. Przypadek ten może wystąpić, gdy w nVision 9 nośnik danych był zablokowany na poziomie Atlasu, użytkownik z Active Directory miał do niego dostęp, ponieważ w nadrzędnym bycie „Active Directory" zdefiniowana była dodatkowa reguła dająca dostęp do tego nośnika.
- Program w wersji 10 traci bezpowrotnie możliwość definiowania reguł DataGuard na poziomie hosta. Tym samym nie jest już możliwe blokowanie i audytowanie użytkowników wyłącznie na wskazanych urządzeniach. Każdy użytkownik ma zawsze ten sam zestaw reguł niezależnie od komputera, na którym aktualnie jest zalogowany.

3. Alarmy

Alarmy nie są w żaden przetwarzane w procesie migracji. W nVision 10, podobnie jak w nVision 9, możliwe jest konfigurowanie alarmów na poziomie ikony urządzenia. Alarmy utworzone w nVision 9 zostaną przeniesione w takiej samej formie na obiekty urządzeń w nowej wersji programu.

4. Raporty

W wyniku migracji danych do nVision 10 utracone zostaną raporty dotyczące informacji o aktywności użytkowników z określonych map lub na wskazanych urządzeniach. Szablony tych raportów nadal będą widoczne w systemie ale wygenerowany przy ich pomocy raport będzie pusty – wynika to z faktu przeniesienia segmentów dotyczących aktywności użytkowników do sekcji raportów generowanych dla grup.
W związku z tym, przed rozpoczęciem procesu migracji należy wykonać potrzebne raporty dla map i urządzeń wg dotychczasowych szablonów, natomiast po migracji należy odtworzyć ręcznie szablony raportów w kontekście grup.

5. Zarządzanie uprawnieniami administratorów

W nVision 10 dane użytkownika zostały przeniesione z bytu w postaci ikony urządzenia na mapach na nowy byt użytkownika w grupach. Ze względu na różnice w działaniu map oraz grup użytkowników, nie jest możliwa migracja ustawień uprawnień administratorów.
W związku z powyższym, jeśli w nVision 9 administrator nie miał uprawnień do wszystkich map, po migracji danych do nVision 10, nie będzie miał uprawnień do żadnej z grup użytkowników.
Niesie to za sobą konieczność ręcznej edycji uprawnień tych administratorów.

6. Powrót do wersji

Uruchomienie instalatora nVision 10 automatycznie wykona kopię zapasową bazy danych nVision 9. Kopia zapasowa zawiera zarówno ustawienia programu oraz dane zebrane w monitorowaniu. Zapisana jest w folderze instalacji nVision w katalogu Backups.
Aby wykonać kopię zapasową ręcznie, należy uruchomić skrót **DBBackup** z folderu **Backups** w ścieżce instalacji serwera nVision (domyślnie: C:\Program Files (x86)\Axence\nVision\Backups).

Aby przywrócić dane z nVision 9:

- Jeśli instalacja nVision 10 nie powiedzie się (lub nie powiedzie się proces migracji), a Serwer nie uruchomi się w nowej wersji to Agenty nie zaktualizują się. W takim przypadku należy:
  - zatrzymać usługę „Axence nVision",
  - usunąć plik **nVision.exe** ze ścieżki instalacji programu na serwerze,
  - pobrać instalator nVision 9 (https://cdn.axence.net/nVision9.zip),
  - zainstalować program,
  - przywrócić kopię zapasową bazy danych poprzez uruchomienie skrótu **DBRestore**.
- Jeśli aktualizacja do nVision 10 powiedzie się a program uruchomi się, Agenty, które podłączyły się do serwera zostaną automatycznie zaktualizowane do najnowszej wersji.
  W tej sytuacji, aby dokonać pełnego downgrade'u do nVision 9 należy:
  - odinstalować Agenty (np. za pomocą polecenia z menu kontekstowego w Konsoli nVision 10),
  - wyłączyć konsolę nVision,
  - zatrzymać usługę „Axence nVision",
  - usunąć plik **nVision.exe** ze ścieżki instalacji programu na serwerze,
  - pobrać instalator nVision 9 (https://cdn.axence.net/nVision9.zip),
  - zainstalować program,
  - przywrócić kopię zapasową bazy danych poprzez uruchomienie skrótu **DBRestore**,
  - ponownie zainstalować Agenty z instalatora skopiowanego z folderu wskazanego po kliknięciu w Konsoli nVision: [menu] **Agenty \ Zainstaluj Agenty nVision.**