

Kontrola dostępu - omówienie

Kontrola dostępu to proces autoryzowania użytkowników, grup i komputerów w celu udostępniania obiektów znajdujących się w sieci lub na komputerze.

Aby poznać działanie kontroli dostępu i zarządzać nią, należy poznać związki między następującymi elementami:

- Obiekty (pliki, drukarki i inne zasoby)
- Tokeny dostępu
- Listy kontroli dostępu (ACL) i wpisy kontroli dostępu (ACE)
- Podmioty (użytkownicy lub aplikacje)
- System operacyjny
- Uprawnienia
- Prawa i uprawnienia użytkowników

Zanim podmiot uzyska dostęp do obiektu, musi zidentyfikować się w podsystemie zabezpieczeń systemu operacyjnego. Informacje o tożsamości są zawarte w tokenie dostępu, który jest tworzony przy każdym logowaniu podmiotu. Przed zezwoleniem podmiotowi na dostęp do obiektu w systemie operacyjnym następuje sprawdzenie, czy token dostępu tego podmiotu ma autoryzację umożliwiającą uzyskanie dostępu do obiektu i wykonanie żadanego zadania. Jest to wykonywane przez porównanie informacji tokenu dostępu z wpisami kontroli dostępu dla obiektu.

Wpisy kontroli dostępu mogą zezwalać na wykonywanie różnych działań w zależności od typu obiektu lub zabraniać ich. Na przykład dla pliku można określić działania Odczyt, Zapis i Wykonywanie. Dla drukarki są dostępne między innymi wpisy Drukowanie, Zarządzanie drukarkami oraz Zarządzanie dokumentami.

Poszczególne wpisy kontroli dostępu dla obiektu są łączone w listę kontroli dostępu. W podsystemie zabezpieczeń następuje wyszukiwanie w liście kontroli dostępu wpisów dotyczących użytkownika lub grup, do których on należy. Każdy kolejny wpis jest sprawdzany, aż zabraknie wpisów lub zostanie znaleziony taki, który zezwala użytkownikowi lub jednej z jego grup na dostęp bądź zabrania go. Jeśli po zbadaniu całej listy żądany dostęp nie został wyraźnie ani dopuszczony, ani zabroniony, następuje odmowa dostępu do obiektu.

Uprawnienia

Uprawnienia definiują typ dostępu udzielanego użytkownikom lub grupom do obiektu lub właściwości obiektu. Na przykład grupie Finanse można udzielić uprawnień Odczyt i zapis do pliku `wynagrodzenia.dat`.

Za pomocą interfejsu użytkownika kontroli dostępu można ustawiać uprawnienia NTFS dla takich obiektów, jak pliki, obiekty usługi Active Directory, obiekty rejestru lub obiekty systemowe, np. procesy. Uprawnień można udzielić dowolnemu użytkownikowi, grupie lub komputerowi. **Dobrym rozwiązaniem jest przypisanie uprawnień do grup**, co zwiększa wydajność systemu podczas weryfikacji dostępu do obiektu.

Do każdego obiektu można udzielić uprawnień:

- Grupom, użytkownikom i innym obiektom mającym identyfikatory zabezpieczeń w domenie.
- Grupom i użytkownikom z domeny oraz z innych zaufanych domen.
- Grupom i użytkownikom lokalnym, utworzonym na komputerze, na którym znajduje się dany obiekt.

Uprawnienia przyłączone do obiektu zależą od typu obiektu. Na przykład uprawnienia, które można przyłączyć do pliku, różnią się od uprawnień, które można przyłączyć do klucza rejestru. Jednak niektóre uprawnienia są wspólne dla większości typów obiektów. Tymi wspólnymi uprawnieniami są:

- Odczyt
- Modyfikowanie
- Zmiana właściciela
- Usuwanie

Podczas ustawiania uprawnień określany jest poziom dostępu dla grup i użytkowników.

Na przykład

- jednemu użytkownikowi można pozwolić na odczytywanie zawartości pliku,
- drugiemu użytkownikowi na wprowadzanie zmian do tego pliku,
- a wszystkim innym użytkownikom zabronić dostępu do tego pliku.

Podobne uprawnienia można ustawiać w odniesieniu do drukarek, tak aby

- określone użytkownicy mogli konfigurować drukarkę,
- a inni mogli tylko na niej drukować.

Aby zmienić uprawnienia do pliku, należy uruchomić Eksploratora Windows, kliknąć prawym przyciskiem myszy nazwę pliku, a następnie kliknąć polecenie **Właściwości**. Na karcie **Zabezpieczenia** można zmienić uprawnienia do pliku.

Uwaga

Inny rodzaj uprawnień, nazywany uprawnieniami udziału, można ustawić na karcie Udostępnianie na stronie Właściwości folderu lub za pomocą kreatora folderów udostępnionych..

Własność obiektów

W momencie tworzenia obiektu jest przypisywany do niego właściciel. Domyślnie właścicielem jest ten użytkownik, który utworzył dany obiekt. Niezależnie od uprawnień ustawionych do obiektu właściciel obiektu może je zawsze zmienić.

Dziedziczenie uprawnień

Dziedziczenie umożliwia administratorom łatwe udzielanie uprawnień i zarządzanie nimi. Funkcja ta powoduje, że obiekty znajdujące się w kontenerze automatycznie dziedziczą uprawnienia tego kontenera. Na przykład pliki znajdujące się w folderze dziedziczą po utworzeniu uprawnienia tego folderu. Dziedziczone są tylko uprawnienia oznaczone jako przeznaczone do dziedziczenia.

Prawa i uprawnienia użytkowników

Prawa użytkowników udzielają określonych uprawnień i praw logowania użytkownikom i grupom w środowisku komputerowym. Administratorzy mogą przypisywać kontom grup lub kontom poszczególnych użytkowników specjalne prawa. Prawa te upoważniają użytkowników do wykonywania określonych akcji, takich jak interakcyjne logowanie się do systemu czy tworzenie kopii zapasowych plików i katalogów.

Prawa użytkowników różnią się od uprawnień, ponieważ prawa użytkowników dotyczą kont użytkowników, podczas gdy uprawnienia są dołączane do obiektów. Chociaż prawa użytkowników można stosować do poszczególnych kont użytkowników, **najlepiej administrować nimi przy użyciu grup**. Interfejs użytkownika kontroli dostępu nie obsługuje udzielania praw poszczególnym użytkownikom. Można jednak administrować prawami użytkowników za pomocą przystawki Zasady zabezpieczeń lokalnych dostępnej w obszarze **Zasady lokalne\Przypisywanie praw użytkownika**.

Inspekcja obiektu

Użytkownik z prawami administratora może przeprowadzać inspekcję zdarzeń związanych z udanym lub nieudanym dostępem do obiektów. Korzystając z interfejsu użytkownika kontroli dostępu, można wybrać obiekty, do których dostęp będzie podlegał inspekcji, ale najpierw należy włączyć zasady inspekcji przez wybranie opcji **Przeprowadź inspekcję dostępu do obiektów** w obszarze **Zasady lokalne\Zasady inspekcji\Zasady lokalne** przystawki Zasady zabezpieczeń lokalnych. Umożliwi to wyświetlanie zdarzeń zabezpieczeń w dzienniku zabezpieczeń Podglądu zdarzeń.

Zarządzanie uprawnieniami

Do każdego kontenera i obiektu w sieci jest dołączony zestaw informacji dotyczących kontroli dostępu. Informacje te, znane jako deskryptory zabezpieczeń, kontrolują typ dostępu przyznany użytkownikom i grupom. Uprawnienia są zdefiniowane w deskrytorze zabezpieczeń obiektu. Uprawnienia są przypisane do określonych grup lub użytkowników.

Użytkownik, który jest członkiem grupy zabezpieczeń skojarzonej z określonym obiektem, ma pewne możliwości w zakresie zarządzania uprawnieniami do tego obiektu. W przypadku obiektów, których jest właścicielem, ma uprawnienia do pełnej kontroli. Istnieją różne metody zarządzania różnymi typami obiektów, takie jak usługi domenowe w usłudze Active Directory (AD DS), zasady grupy czy listy kontroli dostępu.

Uprawnienia i deskryptory zabezpieczeń

Do każdego kontenera i obiektu w sieci jest dołączony zestaw informacji dotyczących kontroli dostępu. Informacje te, znane jako deskryptory zabezpieczeń, kontrolują typ dostępu przyznany użytkownikom i grupom. Deskryptory zabezpieczeń są tworzone automatycznie wraz z tworzeniem kontenerem lub obiektem. Typowym przykładem obiektu z deskryptorem zabezpieczeń jest plik.

Uprawnienia są zdefiniowane w deskrytorze zabezpieczeń obiektu. Uprawnienia są przypisane do określonych grup lub użytkowników. Na przykład wbudowana grupa Administratorzy może mieć w przypadku pliku Temp.dat przypisane uprawnienia Odczyt, Zapis i Usuwanie, podczas gdy grupa Operatorzy kopii zapasowych może mieć przypisane tylko uprawnienia Odczyt i Zapis.

Każde przypisanie uprawnień użytkownikowi lub grupie jest reprezentowane w systemie przez wpis kontroli dostępu. Cały zbiór wpisów uprawnień, znajdujących się w deskrytorze zabezpieczeń, jest nazywany zbiorem uprawnień lub listą kontroli dostępu (ACL, Access Control List). Dlatego do zestawu uprawnień pliku Temp.dat należą dwa wpisy uprawnień - jeden dla wbudowanej grupy Administratorzy, a drugi dla grupy Operatorzy kopii zapasowych.

Uprawnienia jawne a dziedziczone

Dostępne są dwa typy uprawnień: uprawnienia jawne i uprawnienia dziedziczone.

- Uprawnienia jawne to uprawnienia ustawiane domyślnie podczas tworzenia obiektów niebędących obiektami podrzędnymi lub w wyniku działania użytkownika związanego z tymi obiektami, a także z obiektami nadrzędnymi i podrzędnymi.
- Uprawnienia dziedziczone to uprawnienia, które zostały przeniesione na obiekt z obiektu nadrzędnego. Uprawnienia dziedziczone ułatwiają zarządzanie uprawnieniami i zapewniają spójność uprawnień we wszystkich obiektach z wybranego kontenera.


Obiekty tworzone w kontenerze domyślnie dziedziczą uprawnienia z tego kontenera. **Na przykład** po utworzeniu folderu MójFolder wszystkie podfoldery i pliki utworzone w folderze MójFolder automatycznie dziedziczą uprawnienia z tego folderu. Dlatego folder MójFolder ma uprawnienia jawne, podczas gdy wszystkie pliki i podfoldery znajdujące się w nim mają uprawnienia dziedziczone.

Uwaga

Odziedziczone uprawnienia Odmów nie zapobiegają dostępowi do obiektu, jeśli obiekt ma jawny wpis uprawnienia Zezwalaj. Uprawnienia jawne mają wyższy priorytet niż uprawnienia odziedziczone, nawet niż odziedziczone uprawnienia Odmów.

Uprawnienia do plików i folderów

W poniższej tabeli przedstawiono listę ograniczeń dostępu dla każdego zestawu specjalnych uprawnień NTFS.

Uprawnienia specjalne	Pełna kontrola	Modyfikacja	Odczyt i wykonanie	Wyświetlanie zawartości folderu (tylko foldery)	Odczyt	Zapis
Przechodzenie przez folder/Wykonywanie pliku	x	x	x	x		
Wyświetlanie folderu/Odczyt danych	x	x	x	x	x	
Odczyt atrybutów	x	x	x	x	x	
Odczyt atrybutów rozszerzonych	x	x	x	x	x	
Tworzenie plików/Zapis danych	x	x				x
Tworzenie folderów/Dołączanie danych	x	x				x
Zapis atrybutów	x	x				x
Zapis atrybutów rozszerzonych	x	x				x
Usuwanie podfolderów i plików	x					
Usuwanie	x	x				
Odczyt uprawnień	x	x	x	x	x	x
Zmiana uprawnień	x					
Przejęcie na własność	x					
Synchronizowanie	x	x	x	x	x	x
 Ważne <i>Grupy lub użytkownicy, którym udzielono uprawnienia Pełna kontrola do folderu, mogą usuwać z tego folderu dowolne pliki niezależnie od uprawnień chroniących plik.</i>						

Uwagi dodatkowe

- Uprawnienia Wyświetlanie zawartości folderu oraz Odczyt i wykonanie są inaczej dziedziczone, chociaż mają takie same uprawnienia specjalne. Uprawnienie Wyświetlanie zawartości folderu jest dziedziczone przez foldery, a nie przez pliki, i powinno się pojawiać tylko wtedy, gdy użytkownik przegląda uprawnienia do folderu. Uprawnienie Odczyt i wykonanie jest dziedziczone zarówno przez pliki, jak i przez foldery, i jest widoczne zawsze wtedy, gdy użytkownik przegląda uprawnienia do pliku lub do folderu.
- W tej wersji systemu Windows do grupy Wszyscy domyślnie nie należy grupa użytkowników anonimowych, więc uprawnienia udzielone grupie Wszyscy nie mają wpływu na tę grupę.

Uprawnienia udziału i uprawnienia NTFS na serwerze plików

Dostęp do folderu znajdującego się na serwerze plików może zostać określony przez dwa zestawy wpisów uprawnień: zestaw **uprawnień udziału** dotyczących folderu oraz zestaw **uprawnień NTFS** dotyczących folderu (które można również ustawić dla plików). Uprawnienia udziału były często używane do zarządzania komputerami z systemem plików FAT32 lub innymi komputerami, na których nie jest używany system plików NTFS.

Uprawnienia udziału i uprawnienia NTFS są niezależne, co oznacza, że za pomocą jednych nie można modyfikować drugih. Ostateczne uprawnienia dostępu do folderu udostępnionego są definiowane przez uwzględnienie wpisów uprawnienia udziału i uprawnienia NTFS. Następnie **są stosowane uprawnienia bardziej restrykcyjne**.

W poniższej tabeli zaproponowano uprawnienia, których administrator może udzielić grupie Użytkownicy do folderów udostępnionych określonych typów. Można też udzielić uprawnienia udziału Pełna kontrola dla grupy Wszyscy i ograniczać dostęp tylko za pomocą uprawnień NTFS.

Typ folderu	Uprawnienia udziału	Uprawnienia NTFS
Folder publiczny Folder, do którego mają dostęp wszyscy.	Udziel uprawnienia Zmiana grupie Użytkownicy.	Udziel uprawnienia Modyfikacja grupie Użytkownicy.
Folder do wrzucania. Folder, w którym użytkownicy mogą zapisywać zrzut raportów poufnych lub zadania domowe, które może odczytać tylko menedżer grupy lub instruktor.	Udziel uprawnienia Zmiana grupie Użytkownicy. Udziel uprawnienia Pełna kontrola menedżerowi grupy.	Udziel uprawnienia Zapis grupie użytkowników, dla której zastosowano opcję Tylko ten folder (ta opcja jest dostępna na stronie Zaawansowane). Jeśli każdy użytkownik musi mieć określone uprawnienia do zrzutów plików, można utworzyć wpis uprawnienia dla dobrze znanego identyfikatora zabezpieczeń (SID, Security Identifier) twórcy-właściciela i zastosować dla niego opcję Tylko podfoldery i pliki . Można na przykład udzielić uprawnienia Odczyt i zapis do folderu do wrzucania identyfikatorowi SID twórcy-właściciela i zastosować to uprawnienie dla wszystkich podfolderów i plików. Dzięki temu użytkownik, który zrzucił lub utworzył plik (twórca-właściciel), może odczytywać zawartość pliku i zapisywać w nim dane. Twórca-właściciel może uzyskać dostęp do pliku za pomocą polecenia Uruchom z podaniem ścieżki <code>\\NazwaSerwera\FolderDoWrzucania\NazwaPliku</code> . Udziel uprawnienia Pełna kontrola menedżerowi grupy.
Folder aplikacji. Folder zawierający aplikacje, które można uruchamiać za pośrednictwem sieci.	Udziel uprawnienia Odczyt grupie Użytkownicy.	Udziel uprawnień Odczyt, Odczyt i wykonanie oraz Wyświetlanie zawartości folderu grupie Użytkownicy.
Folder domowy. Folder danego użytkownika. Tylko użytkownik ma dostęp do folderu.	Udziel uprawnienia Pełna kontrola do odpowiedniego folderu każdemu użytkownikowi.	Udziel uprawnienia Pełna kontrola do odpowiedniego folderu każdemu użytkownikowi.

Uwagi dodatkowe

- Udzielenie użytkownikowi uprawnienia NTFS Pełna kontrola do folderu umożliwia użytkownikowi przejęcie na własność folderu, o ile użytkownik nie jest zablokowany w inny sposób. Uprawnienia Pełna kontrola należy udzielać ostrożnie.
- Jeżeli chcesz zarządzać dostępem do folderu wyłącznie za pomocą uprawnień NTFS, ustaw dla grupy Wszyscy uprawnienie udziału Pełna kontrola. Nie jest to optymalne rozwiązanie

- **Uprawnienia NTFS** mają wpływ na dostęp lokalny i zdalny. Uprawnienia NTFS obowiązują niezależnie od protokołu. Natomiast **uprawnienia udziału** dotyczą tylko udziałów sieciowych. Uprawnienia udziału nie ograniczają dostępu żadnemu lokalnemu użytkownikowi komputera ani żadnemu użytkownikowi serwera terminali, na którym zostały ustawione uprawnienia udziału. Dlatego uprawnienia udziału nie zapewniają poufności wielu użytkownikom jednego komputera lub serwera terminali.
- Domyślnie do grupy Wszyscy nie należy grupa użytkowników anonimowych, więc uprawnienia udzielone grupie Wszyscy nie mają wpływu na tę grupę.

Uprawnienia dziedziczone

Uprawnienia dziedziczone to uprawnienia, które zostały przeniesione na obiekt z obiektu nadrzędnego. Uprawnienia dziedziczone ułatwiają zarządzanie uprawnieniami i zapewniają spójność uprawnień we wszystkich obiektach z wybranego kontenera.

Dziedziczenie dla wszystkich obiektów

Jeśli podczas przeglądania uprawnień dla obiektu pola wyboru uprawnień **Zezwalaj** i **Odmów** znajdujące się w różnych częściach interfejsu użytkownika kontroli dostępu są zacieniowane, oznacza to, że obiekt odziedziczył uprawnienia z obiektu nadrzędnego. Odziedziczone uprawnienia można ustawić przy użyciu karty **Uprawnienia** strony właściwości **Zaawansowane ustawienia zabezpieczeń**.

Istnieją trzy zalecane sposoby wprowadzania zmian w uprawnieniach dziedziczonych:

- Wprowadzenie zmian w obiekcie nadrzędnym, w którym uprawnienia zostały zdefiniowane jawnie - obiekt podrzędny odziedziczy te uprawnienia
- Zaznaczenie uprawnienia **Zezwalaj**, aby zastąpić dziedziczone uprawnienie **Odmów**.
- Wyczyszczenie pola wyboru **Dołącz uprawnienia dziedziczone z tego obiektu nadrzędnego**. Następnie można wprowadzać zmiany w uprawnieniach bądź usunąć użytkowników lub grupy z listy **Uprawnienia**. Jednak obiekt nie będzie już wtedy dziedziczyć uprawnień po obiekcie nadrzędnym.

Uwaga

Odziedziczone uprawnienia Odmów nie zapobiegają dostępowi do obiektu, jeśli obiekt ma jawny wpis uprawnienia Zezwalaj.

Uwaga

Uprawnienia jawne mają wyższy priorytet niż uprawnienia odziedziczone, nawet niż odziedziczone uprawnienia Odmów.
