TECHNOLOGIA

AUTOMATYZACJA ZARZĄDZANIA PODATNOŚCIAMI SYSTEMÓW INFORMATYCZNYCH POPRZEZ WYKORZYSTANIE CHMUROWEJ USŁUGI MICROSOFT AZURE UPDATE MANAGEMENT W SYSTEMACH MICROSOFT I LINUX

mgr inż. Adam Jakubiec
inż. Bogusław Gacek

magazyn.wsei.edu.pl

Streszczenie

Artykuł dotyczy usługi chmurowej Azure Update Manager. Narzędzie to daje możliwość automatyzacji instalowania poprawek systemowych zapewniając nie tylko wyższy stopień aktualności systemów, ale przede wszystkim szybszą likwidację luk w zabezpieczeniach systemów operacyjnych poprzez implementowanie poprawek z kategorii „security" bez zbędnej zwłoki. To podejście w znacznym stopniu przyczynia się do zwiększenia poziomu bezpieczeństwa środowisk Windows i Linux występujących w warunkach wielochmurowych, a także w formie maszyn wirtualnych, czy na zwykłych komputerach użytkowników. Niniejsza publikacja stara się wziąć pod uwagę wszelkie argumenty za i przeciw implementacji tego typu rozwiązania, które przed napisaniem artykułu zostało przetestowane od strony praktycznej w dedykowanym środowisku testowym odzwierciedlającym warunki panujące w typowych organizacjach.

SŁOWA KLUCZOWE

Chmura, zarządzanie bezpieczeństwem, poprawki systemowe, automatyzacja, aktualizacje, Azure, Windows, Linux.

Wprowadzenie

Regularne aktualizowanie systemów operacyjnych w kontekście usuwania znanych luk bezpieczeństwa stanowi wyzwanie dla działów IT. Klasyczne podejście do tego zagadnienia – ręczne instalowanie poprawek – jest zadaniem czasochłonnym ze względu na czas trwania, konieczność spełnienia zależności i fakt samej wydajności sprzętowej pozostawiającej wiele do życzenia w poruszanym zakresie. Z punktu widzenia zarządzania cyberbezpieczeństwem utrzymywanie systemów produkcyjnych w stanie jak najbardziej aktualnym stanowi podstawowy wymóg wielu regulacji, zaleceń i dobrych praktyk.

Artykuł ma za zadanie odpowiedzieć na pytanie, czy automatyzacja instalacji poprawek ma uzasadnienie w środowisku produkcyjnym, czy implementacja automatyzacji ma uzasadnienie, jakie niesie korzyści oraz potencjalne zagrożenia? Inwentaryzacja stanu instalacji poprawek systemowych oraz instalacja w oparciu o harmonogramy oraz możliwość ręcznego wymuszenia z centralnej konsoli będzie realizowana za pomocą usługi Microsoft Update Manager o charakterze chmurowym, jednakże uwzględnia możliwości zarządzania poprawkami w środowisku hybrydowym – maszyny hostowane w chmurze oraz serwery znajdujące się także lub tylko w lokalnych centrach danych i stacje robocze (również te które są rozproszone) znajdują się poza lokalizacją firmy, a jedyny wymóg to dostęp do Internetu oraz wcześniejsza rejestracja w usłudze.

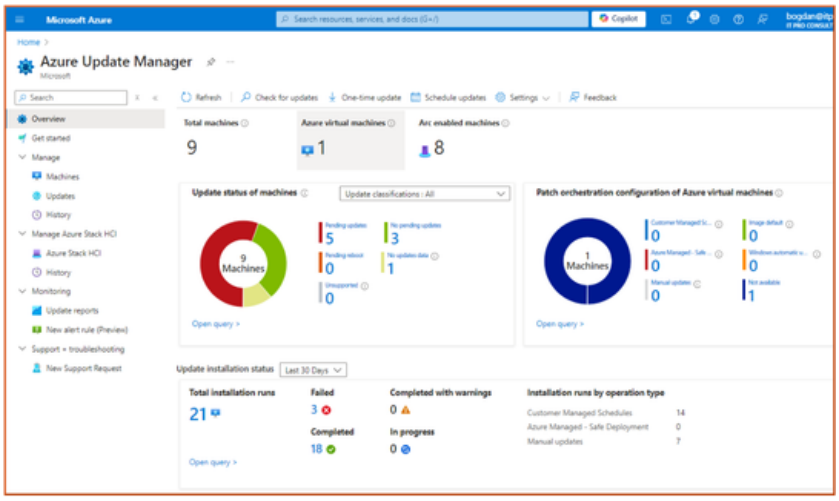
Zasadniczy opis usługi Azure Update Manager

Azure Update Manager obsługuje szeroki zakres środowisk – Windows, Linux, VMWare, SCVMM oraz maszyny wirtualne rozwiązania Azure Stack HCI. Dzięki temu organizacje mogą zarządzać aktualizacjami w zróżnicowanych środowiskach z jednej przejrzystej konsoli. Usługa oferuje elastyczne opcje planowania aktualizacji, umożliwiając natychmiastowe wdrażanie aktualizacji, planowanie ich na określony czas lub automatyczne aktualizowanie poza godzinami pracy. Użytkownicy mogą synchronizować cykle poprawek z harmonogramami konserwacji, oknami serwisowymi, co minimalizuje przestoje i zakłócenia w pracy systemów. Usługa oferuje zaawansowane narzędzia do raportowania i monitorowania stanu aktualizacji. Administratorzy mogą tworzyć niestandardowe pulpity nawigacyjne, konfigurować alerty oraz monitorować zgodność aktualizacji dla całej farmy maszyn. Dzięki temu możliwe jest szybkie reagowanie na potencjalne zagrożenia i utrzymanie wysokiego poziomu bezpieczeństwa. Usługa może stanowić kluczowy element strategii zarządzania aktualizacjami w nowoczesnych organizacjach.

Wdrożenie usługi Azure Update Management

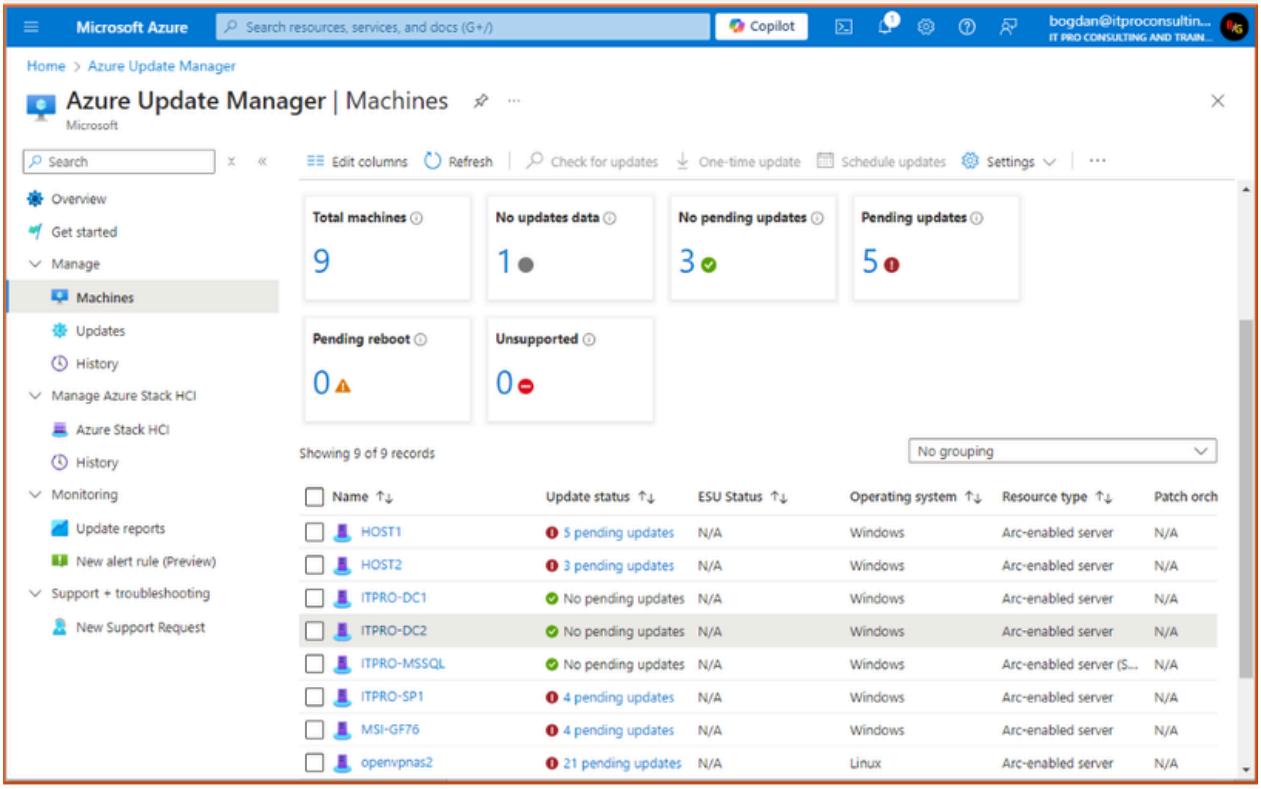
Wdrożenie zarządzania poprawkami przy pomocy omawianego narzędzia w środowisku chmurowym jest procesem, nieskomplikowanym polegającym w zasadzie na włączeniu tej opcji z poziomu maszyny, jednakże w przypadku lokalnych serwerów i stacji roboczych konieczna jest rejestracja systemów operacyjnych za pomocą usługi Azure Arc. Jest to rozwiązanie, które umożliwia zarządzanie zasobami IT w środowiskach hybrydowych i wielochmurowych. W połączeniu z usługą Azure Update Manager, Azure Arc pozwala na centralne zarządzanie aktualizacjami systemów operacyjnych niezależnie od ich lokalizacji. Konfiguracja Azure Arc może odbywać się na kilka sposobów – bezpośrednio z serwerowego systemu operacyjnego (począwszy od wersji Windows Server 20221), skryptem dedykowanym dla urządzenia z systemem operacyjnym Microsoft lub Linux, a także skryptami przeznaczonymi do masowej rejestracji urządzeń z wykorzystaniem zasad polityk grupowych (GPO) lub urządzeń mobilnych zarządzanych za pomocą narzędzia MDM Microsoft Intune.

Korzystanie z usługi Azure Arc jest darmowe (podczas gdy korzystanie z funkcji Menedżera Aktualizacji Azure łączy się z miesięcznym kosztem opłaty subskrypcyjnej od każdego zarządzanego obiektu). Wg aktualnie obowiązującego cennika (wrzesień 2024) kwota ta wynosi 5 USD.



RYS.1. WIDOK NA KONSOLE AZURE UPDATE MANAGER

AZURE UPDATE MANAGER UMOŻLIWIA ZARZĄDZANIE AKTUALIZACJAMI W ZRÓŻNICOWANYCH ŚRODOWISKACH, TAKICH JAK WINDOWS, LINUX, VMWARE I AZURE STACK HCI, Z JEDNEJ PRZEJRZYSTEJ KONSOLI, OFERUJĄC ELASTYCZNE OPCJE PLANOWANIA AKTUALIZACJI ORAZ ZAAWANSOWANE NARZĘDZIA DO MONITOROWANIA I RAPORTOWANIA.

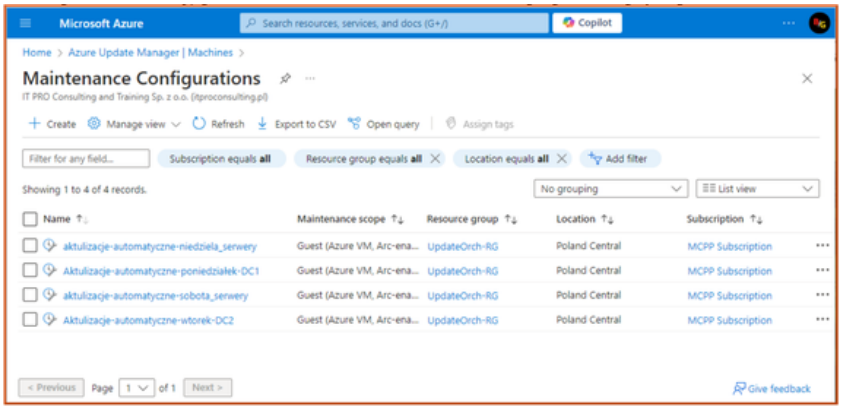


RYS.2. WIDOK NA KONSOLE AZURE UPDATE MANAGER

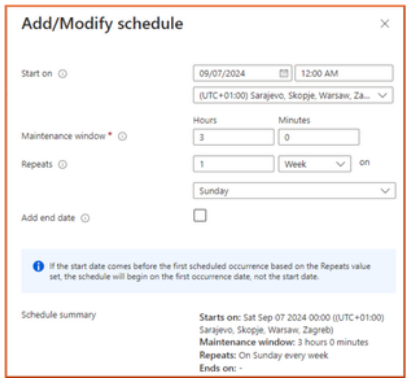
Planowanie i konfiguracja usługi

Przed skonfigurowaniem usługi należy przemyśleć i zaplanować harmonogram aktualizacji. W trakcie formowania tego planu należy określić zasoby krytyczne, które nie podlegają aktualizacjom automatycznym – mogą to być fizyczne hosty Hyper-V, infrastruktura krytyczna wymagająca każdorazowej weryfikacji funkcjonalności po instalowaniu poprawek oraz maszyny, dla których nie można z różnych względów ustalić stałego harmonogramu aktualizacji. Z takiego harmonogramu już na późniejszym etapie wyklucza się automatyczną instalację poprawek na serwerach, na których zdiagnozowano problemy podczas instalacji.
Godzinowy harmonogram aktualizacji również powinien być skrupulatnie przemyślany i w miarę potrzeb modyfikowany, gdyż przykładowo nie będzie do dobrych praktyk zaliczana sytuacja, gdy duża ilość maszyn aktualizowana jest w tym samym czasie. W przypadku maszyn pełniących tę samą funkcję – przykładowo redundantne kontrolery domeny – nie ma mowy o równoległym aktualizowaniu. Takie maszyny należy przydzielić do harmonogramów zaplanowanych na różne dni.

Istotną kwestią jest również włączenie automatycznej oceny stanu instalacji poprawek na urządzeniach końcowych. Opcja ta nie jest skonfigurowana domyślnie i bez ręcznego zainicjowania zbierania tych informacji nie byłoby możliwe poznanie statusu środowiska. Nadmienić należy, że informacje zbierane automatycznie spływają z opóźnieniem. Warto zwrócić uwagę na sprawdzanie stanu poszczególnych punktów końcowych w sytuacji wątpliwej.



RYS.3. HARMONOGRAMY UŁUGI AZURE UPDATE MANAGER

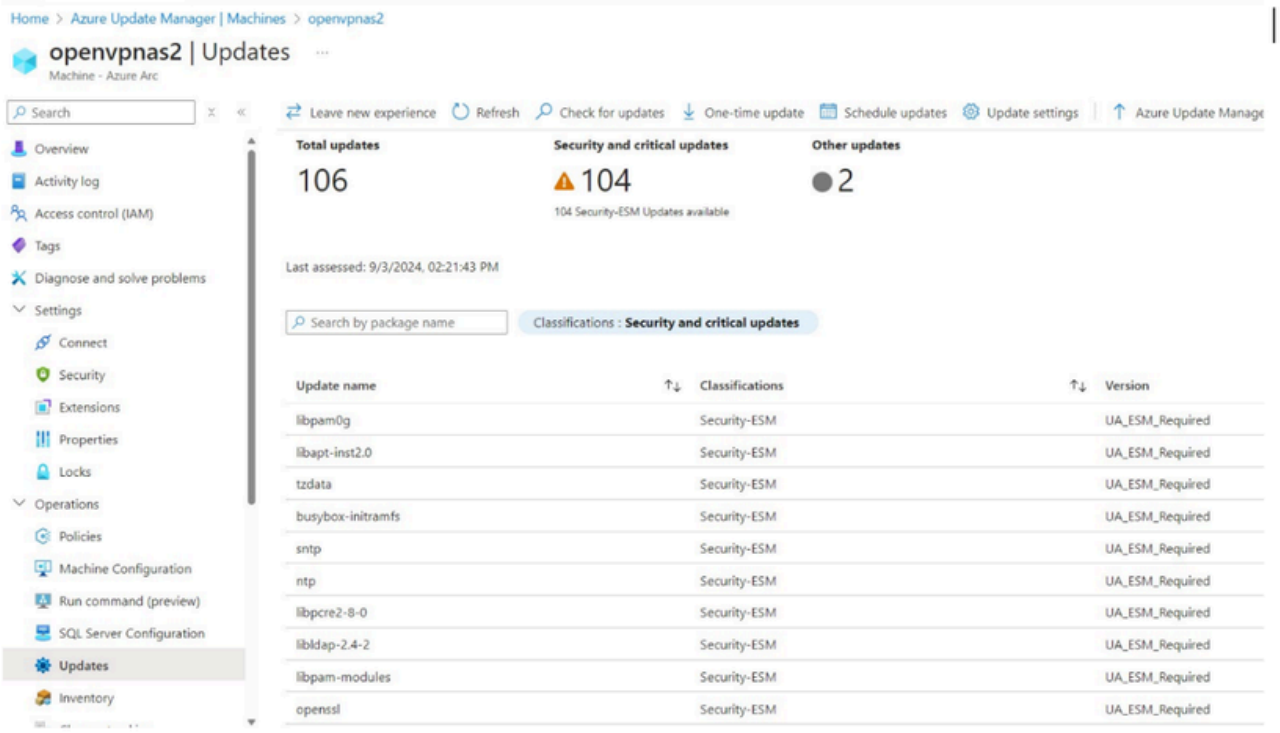


RYS.4. EDYTOR HARMONOGRAMU

Zidentyfikowane wady rozwiązania

Podczas eksploatacji rozwiązania w środowisku testowym zidentyfikowano szereg niedogodności.

W starszych dystrybucjach Linux widocznych jest wiele poprawek zaklasyfikowanych do kategorii Security, jednak próba ich instalacji kończy się niepowodzeniem. Aktualizacja dystrybucji Linux do najnowszej wersji pozwalała na dalszą implementację poprawek, aczkolwiek w dalszym ciągu pozostawała pewna pula poprawek, których próba instalacji kończyła się niepowodzeniem.



RYS.5. INFORMAJCA O ZNACZNEJ ILOŚCI NIEZAINSTALOWANYCH POPRAWEK KLASYFIKOWANYCH JAKO SECURITY E SM, W STARSZEJ DYSTRYBUCJI SYSTEMU LINUX

Od jakiegoś czasu usługa Windows Update oferuje możliwość aktualizacji sterowników w ramach kategorii poprawek dodatkowych. W systemie Azure Update Manager poprawki tej kategorii są widoczne, aczkolwiek ich instalacja z poziomu usługi chmurowej nie jest obsługiwana. Wiąże się to z koniecznością instalowania tego typu poprawek z poziomu indywidualnego urządzenia.

Rysunek: niewspierane kategorie poprawek sprzętowych są widoczne w wykazie, aczkolwiek ich instalacja nie jest możliwa z poziomu Azure Update Manager.

Kolejną wadą, a właściwie niedociągnięciem, do którego administratorzy i pracownicy działu technicznego muszą się przyzwyczaić jest brak synchronizacji pomiędzy historią zainstalowanych poprawek. Poprawki instalowane z poziomu Azure Update Managera nie są widoczne w lokalnej historii poprawek i na odwrót – w przypadku, gdy z jakiegoś powodu poprawki implementowane są ręcznie na poziomie systemu operacyjnego – śladu takiej aktywności nie widać w panelu usługi chmurowej. Status określający potrzebne poprawki oczywiście nie będzie uwzględniał tych zainstalowanych lokalnie na poziomie urządzenia.

Podsumowanie

Microsoft Azure Manager to zaawansowane narzędzie do zarządzania aktualizacjami systemowymi z centralnego miejsca w chmurze, które oferuje szeroki wachlarz możliwości (w tym raportowanie i możliwość automatyzacji tego procesu oraz ograniczenie zaległości w spełnieniu tego wymagania, co przekłada się bezpośrednio na większy stopień zabezpieczeń firmowych systemów informatycznych). Może stanowić centralny punkt raportowania w środowiskach rozproszonych. Pomimo wielu zalet rozwiązanie nie jest pozbawione wad. Takich jak powtarzalny koszt subskrypcyjny zależny od ilości urządzeń znajdujących się w zarządzanym zakresie. Koszt ten wydaje się być akceptowalny, gdyż stanowi remedium na zdjęcie z (i tak już przeciążonymi obowiązkami pracowników działu IT). Należy pamiętać, że nie wszystkie (szczególnie kluczowe obiekty) podlegają automatyzacji – szczególnie należy rozważyć przypadki elementów kluczowych infrastruktury, gdzie forsowanie automatyzacji poprawek kosztem potencjalnych zaburzeń w dostępności usługi stanowiłoby zbyt duże ryzyko. Zresztą zanim osiągnięty zostanie wysoki stopień automatyzacji, konieczne jest odpowiednie zaplanowanie i przetestowanie wdrożenia.

Referencje i odnośniki

https://learn.microsoft.com/pl-pl/azure/update-manager/overview
https://azurearcjumpstart.com/azure_arc_jumpstart/azure_arc_servers/day2/arc_updateManagementCenter

https://learn.microsoft.com/pl-pl/azure/update-manager/workflow-update-manager?tabs=azure-vms%2Cupdate-win

Bibliografia

1. J. C. Andersson, *Learning Microsoft Azure: Cloud Computing and Development Fundamentals,* 1st ed., Sebastopol, CA, USA: O'Reilly Media, 2023, pp. 374.
2. I. Foulds, *Learn Azure in a Month of Lunches, Second Edition*, Shelter Island, NY, USA: Manning Publications Co., 2020, pp. 241–248.