Sandbox dla Windows

Windows Sandbox to izolowane, tymczasowe środowisko pulpitu, w którym można uruchamiać niezaufane oprogramowanie bez obawy o złośliwe narażenie na działanie komputera. Windows Sandbox obsługuje teraz proste pliki konfiguracyjne (rozszerzenie .wsb), które zapewniają minimalną obsługę skryptów. Możesz użyć tej funkcji w najnowszej wersji systemu Windows o numerze 18342.

Wszelkie oprogramowanie zainstalowane w piaskownicy systemu Windows pozostaje tylko w piaskownicy i nie może wpływać na urządzenie. Po zamknięciu piaskownicy systemu Windows całe zainstalowane oprogramowanie ze wszystkimi jego plikami i statusem jest trwale usuwane.

Windows Sandbox ma następujące właściwości:

1. Część systemu Windows - Wszystko, czego potrzebujesz do tej funkcji, jest domyślnie dostępne w Windows Pro i Enterprise. Nie ma potrzeby pobierania VHD!
2. Czystość - za każdym razem, gdy uruchamia się Windows Sandbox, jest tak czysty, jak nowa instalacja systemu Windows
3. Jednorazowe - nic nie jest zapisywane na urządzeniu; wszystko jest usuwane po zamknięciu aplikacji
4. Bezpieczne - używa wirtualizacji sprzętowej do izolowania jądra, które korzysta z hiperwizora Microsoft do uruchamiania osobnego jądra izolującego Windows Sandbox od hosta
5. Skuteczne - korzysta ze zintegrowanego harmonogramu jądra, inteligentnego zarządzania pamięcią i wirtualnego GPU

Pliki konfiguracji piaskownicy systemu Windows.

Pliki konfiguracyjne piaskownicy są w formacie XML i są powiązane z plikiem piaskownicy z rozszerzeniem .wsb. Plik konfiguracyjny pozwala użytkownikowi kontrolować następujące aspekty piaskownicy systemu Windows:

1. vGPU (zwirtualizowany procesor graficzny)
Włącz lub wyłącz zwirtualizowany procesor graficzny. Jeśli vGPU jest wyłączone, Sandbox użyje WARP (rasterizer oprogramowania).
2. Sieć
Włącz lub wyłącz dostęp sieciowy do piaskownicy.

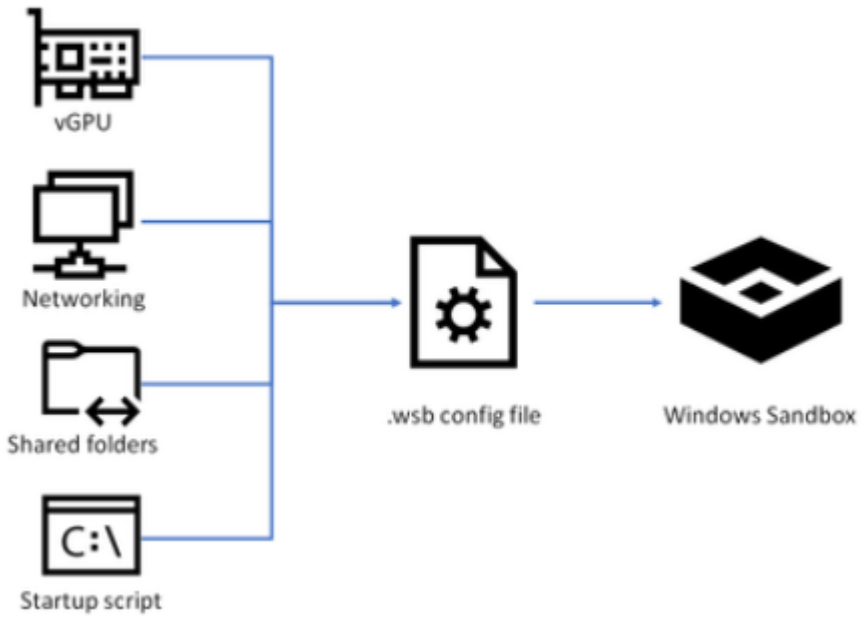
3. Foldery udostępnione

Udostępniaj foldery z hosta (komputera) z uprawnieniami do odczytu lub zapisu. Należy pamiętać, że rozszerzenie katalogów hosta może pozwolić złośliwemu oprogramowaniu wpływać na system lub kraść dane.

4. Uruchamianie skryptu

Automatyczne działanie po wejściu do piaskownicy.

Akcja logowania do piaskownicy.



Obsługiwane opcje konfiguracji

vGPU - Procesor wirtualny

Włącza lub wyłącza udostępnianie GPU.

<vGPU>value</vGPU>

Obsługiwane wartości:

Włącz: włącza obsługę procesora vGPU w piaskownicy.

Wyłącz - wyłącz obsługę vGPU w piaskownicy. Jeśli ta wartość zostanie ustawiona, użyje renderowania programowego, które może być wolniejsze niż zwirtualizowany procesor graficzny.

Domyślnie - jest to domyślna wartość dla obsługi vGPU; oznacza to, że vGPU jest włączone.

Uwaga: Włączenie zwirtualizowanego GPU może potencjalnie zwiększyć atak zewnętrznego piaskownicy.

Sieć

Włącza lub wyłącza sieć w piaskownicy. Wyłączenie dostępu do sieci może być wykorzystane do zmniejszenia prawdopodobieństwa ataku piaskownicy.

<Networking>value</Networking>

Obsługiwane wartości:

Włącz: włącza sieć w piaskownicy.

Wyłącz - wyłącz sieć w piaskownicy.

Domyślnie - jest to domyślna wartość dla obsługi sieci. Umożliwia tworzenie sieci poprzez utworzenie przełącznika wirtualnego na hoście i połączenie z nim izolowanego środowiska programowego za pośrednictwem wirtualnej karty sieciowej.

Uwaga: Włączenie połączeń sieciowych może spowodować, że niezaufane aplikacje znajdą się w sieci wewnętrznej.

Mapowane foldery

Zawiera listę obiektów MappedFolder.

Mapowany folder Określa pojedynczy folder na komputerze hosta, który zostanie udostępniony na pulpicie kontenera. Aplikacje w trybie piaskownicy działają na koncie użytkownika „WDAGUtilityAccount". Dlatego wszystkie foldery są wyświetlane w następującej ścieżce: C:\Users\WDAGUtilityAccount\Desktop.

Na przykład „C:\Test" pojawi się jako „C:\Users\WDAGUtilityAccount\Desktop\Test".

Tablica folderów, z których każdy reprezentuje lokalizację na komputerze hosta, która jest współużytkowana z piaskownicą w określonej ścieżce. W tej chwili ścieżki względne nie są obsługiwane. Jeśli ścieżka nie zostanie określona, folder zostanie zamapowany na pulpit użytkownika kontenera.

<MappedFolders>

<MappedFolder>

<HostFolder>absolute path to the host folder</HostFolder>

<SandboxFolder>absolute path to the sandbox folder</SandboxFolder>

```
  <ReadOnly>value</ReadOnly>
 </MappedFolder>
 <MappedFolder>
  ...
 </MappedFolder>
</MappedFolders>
```

HostFolder: określa folder na komputerze hosta, który ma zostać udostępniony w obszarze izolowanym. Folder musi już istnieć na hoście, w przeciwnym razie uruchomienie kontenera nie powiedzie się.

SandboxFolder: Określa miejsce docelowe w obszarze izolowanym, do którego ma zostać zamapowany folder. Jeśli folder nie istnieje, zostanie utworzony. Jeśli nie określono folderu piaskownicy, folder jest mapowany na pulpit kontenera.

ReadOnly: Jeśli true, wymusza dostęp tylko do odczytu do folderu udostępnionego z poziomu kontenera. Obsługiwane wartości: prawda/fałsz. Wartość domyślna to false. Obsługiwane wartości: prawda / fałsz.

Uwaga: Pliki i foldery powiązane z hostem mogą zostać naruszone przez aplikacje w piaskownicy lub potencjalnie wpłynąć na hosta.

Polecenie logowania

Określa jedno polecenie, które zostanie wywołane automatycznie po wejściu do kontenera.

Zespół: Ścieżka do pliku wykonywalnego lub skryptu w kontenerze, który zostanie wykonany po zalogowaniu. Aplikacje w piaskownicy są uruchamiane w ramach konta użytkownika kontenera. Konto użytkownika kontenera powinno być kontem administratora.

```
<LogonCommand>
 <Command>command to be invoked</Command>
</LogonCommand>
```

Polecenie: ścieżka do pliku wykonywalnego lub skryptu wewnątrz kontenera, który zostanie wykonany po zalogowaniu.

Wejście audio

Udostępnia wejście mikrofonu hosta w piaskownicy.

Włącza lub wyłącza wejście audio do piaskownicy.

<AudioInput>value</AudioInput>

Obsługiwane wartości:

Włącz: Włącza wejście audio w piaskownicy. Jeśli ta wartość jest ustawiona, obszar izolowany może odbierać dane wejściowe audio od użytkownika. Aplikacje korzystające z mikrofonu mogą wymagać tej funkcji.

Wyłącz: Wyłącza wejście audio w piaskownicy. Jeśli ta wartość jest ustawiona, piaskownica nie może odbierać danych wejściowych audio od użytkownika. Aplikacje korzystające z mikrofonu mogą nie działać prawidłowo z tym ustawieniem.

Domyślnie: Ta wartość jest wartością domyślną obsługi wejścia audio. Obecnie ta wartość domyślna oznacza, że wejście audio jest włączone.

Wejście wideo

Udostępnia wejście z kamery internetowej hosta w piaskownicy.

Włącza lub wyłącza wejście wideo do piaskownicy.

<VideoInput>value</VideoInput>

Obsługiwane wartości:

Włącz: Włącza wejście wideo w piaskownicy.

Wyłącz: Wyłącza wejście wideo w piaskownicy. Aplikacje korzystające z wejścia wideo mogą nie działać poprawnie w piaskownicy.

Domyślnie: Ta wartość jest wartością domyślną obsługi wejścia wideo. Obecnie ta wartość domyślna oznacza, że wejście wideo jest wyłączone. Aplikacje korzystające z wejścia wideo mogą nie działać poprawnie w piaskownicy.

Chroniony klient

Umieszcza zwiększone ustawienia zabezpieczeń w sesji protokołu RDP (Remote Desktop Protocol) w piaskownicy.

Gdy tryb klienta chronionego jest włączony, piaskownica dodaje nową warstwę granicy zabezpieczeń, uruchamiając ją w środowisku wykonawczym izolacji AppContainer.

Izolacja AppContainer zapewnia izolację poświadczeń, urządzeń, plików, sieci, procesów i okien.

<ProtectedClient>value</ProtectedClient>

Obsługiwane wartości:

Włącz: uruchamia piaskownicę systemu Windows w trybie klienta chronionego. Jeśli ta wartość jest ustawiona, piaskownica jest uruchamiana w izolacji AppContainer.

Wyłącz: Uruchamia piaskownicę w trybie standardowym bez dodatkowych środków zaradczych.

Wartość domyślna: Ta wartość jest wartością domyślną dla trybu klienta chronionego. Obecnie ta wartość domyślna oznacza, że piaskownica nie działa w trybie klienta chronionego.

Przekierowanie drukarki

Udostępnia drukarki z hosta do piaskownicy.

Włącza lub wyłącza udostępnianie drukarki z hosta do obszaru izolowanego.

<PrinterRedirection>value</PrinterRedirection>

Obsługiwane wartości:

Włącz: Umożliwia udostępnianie drukarek hosta w obszarze izolowanym.

Wyłącz: Wyłącza przekierowywanie drukarki w piaskownicy. Jeśli ta wartość jest ustawiona, piaskownica nie może wyświetlać drukarek z hosta.

Domyślnie: Ta wartość jest wartością domyślną obsługi przekierowywania drukarki. Obecnie ta wartość domyślna oznacza, że przekierowanie drukarki jest wyłączone.

Przekierowanie schowka

Udostępnia schowek hosta piaskownicy, dzięki czemu tekst i pliki mogą być wklejane tam iz powrotem.

Włącza lub wyłącza udostępnianie schowka hosta w obszarze izolowanym.

<ClipboardRedirection>value</ClipboardRedirection>

Obsługiwane wartości:

Włącz: Umożliwia udostępnianie schowka hosta w piaskownicy.

Wyłącz: Wyłącza przekierowanie schowka w piaskownicy. Jeśli ta wartość jest ustawiona, kopiowanie/wklejanie do i z obszaru izolowanego jest ograniczone.

Ustawienie domyślne: Ta wartość jest wartością domyślną przekierowania schowka. Obecnie kopiowanie/wklejanie między hostem a piaskownicą jest dozwolone w obszarze domyślnym.

Pamięć w MB

Ilość pamięci (w megabajtach) do przypisania do piaskownicy.

```
<MemoryInMB>value</MemoryInMB>
```

Jeśli podana wartość pamięci jest niewystarczająca do uruchomienia piaskownicy, jest ona automatycznie zwiększana do wymaganej wartości minimalnej.

Uwaga: Chociaż będą działać bardzo proste polecenia (uruchamianie pliku wykonywalnego lub skryptu), bardziej złożone skrypty, zawierające kilka kroków, powinny zostać umieszczone w pliku skryptu. Ten plik skryptu można zmapować do kontenera poprzez folder współdzielony, a następnie wykonać przy użyciu dyrektywy LogonCommand.

Plik konfiguracyjny

Przykładowy plik tekstowy Downloads.wsb z rozszerzeniem .wsb.

```
<Configuration>
 <vGpu>Disable</vGpu>
 <Networking>Disable</Networking>
 <MappedFolders>
  <MappedFolder>
   <HostFolder>C:\Users\Public\Downloads</HostFolder>
   <SandboxFolder>C:\Users\WDAGUtilityAccount\Downloads</SandboxFolder>
   <ReadOnly>true</ReadOnly>
  </MappedFolder>
 </MappedFolders>
```

```
  <LogonCommand>
    <Command>explorer.exe C:\users\WDAGUtilityAccount\Downloads</Command>
  </LogonCommand>
</Configuration>
```

Klikasz dwukrotnie utworzony plik * .wsb otwierasz go w piaskownicy systemu Windows.