

Implementación del acceso a máquinas virtuales Just-In-Time



El acceso a máquinas virtuales (VM) Just-In-Time (JIT) se usa para bloquear el tráfico entrante a las máquinas virtuales de Azure, lo que reduce la exposición a ataques y, al mismo tiempo, proporciona acceso sencillo para conectarse a las máquinas virtuales cuando sea necesario.

Tras habilitar el acceso a máquinas virtuales Just-In-Time, creará una directiva que determine los puertos que se van a proteger, cuánto tiempo deben permanecer abiertos estos puertos y las direcciones IP aprobadas que pueden acceder a estos puertos. La directiva ayuda a mantener el control de lo que los usuarios pueden hacer cuando solicitan acceso. Las solicitudes se registran en el registro de actividad de Azure, de tal modo que se pueda supervisar y auditar fácilmente el acceso. La directiva también ayudará a identificar rápidamente las máquinas virtuales existentes que tienen habilitado el Acceso a VM Just-In-Time y las máquinas virtuales en las que se recomienda este tipo de acceso.

Funcionamiento del acceso a máquinas virtuales JIT

Para acceder a máquinas virtuales Just-In-Time, debe habilitar Microsoft Defender para la nube.







Inicio > [Security Center](#) > Configuración


 Configuración de planes de Azure Defender 

ASC DEMO

Configuración

1 Planes de Azure Defender

-  Recopilación de datos
-  Notificaciones por correo electrónico
-  Detección de amenazas
-  Automatización de flujos de trabajo
-  Exportación continua
-  Conectores en la nube (versión preliminar)

 Azure Defender proporciona seguridad mejorada. [Más información](#)

Azure Defender está desactivado.	Azure Defender está activado.
✓ Evaluación continua y recomendaciones de seguridad	✓ Evaluación continua y recomendaciones de seguridad
✓ Puntuación de seguridad de Azure	✓ Puntuación de seguridad de Azure
✗ Acceso a VM Just-In-Time	✓ Acceso a VM Just-In-Time
✗ Controles de aplicaciones adaptables y refuerzo de redes	✓ Controles de aplicaciones adaptables y refuerzo de redes
✗ Panel de cumplimiento normativo e informes	✓ Panel de cumplimiento normativo e informes
✗ Protección contra amenazas para máquinas virtuales de Azure y sistemas híbridos (incluido servidor EDR)	✓ Protección contra amenazas para máquinas virtuales de Azure y sistemas híbridos (incluido servidor EDR)
✗ Protección contra amenazas para los servicios PaaS admitidos	✓ Protección contra amenazas para los servicios PaaS admitidos

Después de habilitar Defender, puede ver qué máquinas virtuales tienen JIT configurado. Habilite JIT en cualquier máquina virtual que no tenga un estado correcto.

Inicio > [Security Center](#) >

Acceso de máquina virtual Just-In-Time

Máquinas virtuales

Configurado No configurado No compatible

Para que el Centro de Seguridad restrinja el acceso a sus puertos de administración, active el control de acceso a todas sus máquinas virtuales de riesgo "alto" y "bajo". JIT es innecesario en una máquina virtual "en buen estado".

[Habilitar JIT en 1 VM](#)

	Máquina virtual T4	Grupo de recursos T4	Nombre de la suscripción T4	Gravedad
<input type="checkbox"/>	 ArikostCreateTest	ASCDemo	DEMOSTRACIÓN DE ASC	 Correcto
<input type="checkbox"/>	 YoafriVM	ANAT_TEST_RG	DEMOSTRACIÓN DE ASC	 P-ATO de J
<input checked="" type="checkbox"/>	 vm1	ASCDemORG	DEMOSTRACIÓN DE ASC	 P-ATO de J
<input type="checkbox"/>	 Barracuda	CONTOSOWEB	DEMOSTRACIÓN DE ASC	 P-ATO de JA

Para cada máquina virtual, se recomienda un acceso y puertos específicos.

Inicio > [Security Center](#) > [Acceso de máquina virtual Just-In-Time](#)

Configuración de acceso Just-In-Time a la máquina virtual

vm1

[+](#) [Agregar](#) [Guardar](#) [X](#) [Descartar](#)

Configure los puertos a los que se aplicará el acceso a Just-in-Time a la máquina virtual

Puerto	Protocolo	Direcciones IP de origen permitidas	Intervalo de tiempo (horas)
22 (Recomendado)	Cualquiera	Por solicitud	No procede
3389 (Recomendado)	Cualquiera	Por solicitud	No procede
5985 (Recomendado)	Cualquiera	Por solicitud	No procede
5986 (Recomendado)	Cualquiera	Por solicitud	No procede

Puede aceptar las recomendaciones o **agregar** otros puertos.

Adición de configuración de puerto

Puerto*

Protocolo

Cualquier

TCP

UDP

Direcciones IP de origen permitidas

Por solicitud

Bloque CIDR

Direcciones IP ⓘ

Tiempo máximo de solicitud



3

(horas)

Descartar

Aceptar

Una vez que todo esté en su lugar, los usuarios deberán solicitar acceso a la máquina virtual. También puede supervisar el uso de cada máquina virtual.

Máquinas virtuales

Configurado Sin configurar No compatible

VM para las que ya se ha aplicado el control de acceso a VM Just-In-Time. Los datos mostrados son de la semana pasada.

19 Máquinas virtuales

vm					
Máquina virtual ↑↓	Aprobado	Último acceso ↑↓	Detalles de conexión	Último usuario ↑↓	
<input checked="" type="checkbox"/> Máquina virtual	0 solicitudes	N/D	-	N/D	...
<input type="checkbox"/> PE-vm	0 solicitudes	N/D	-	N/D	...

Solicitar acceso

Revocar acceso

Para más información, consulte [Protección de los puertos de administración con acceso Just-In-Time](#).

Bloquee el tráfico entrante a sus Azure Virtual Machines con la función de acceso a máquinas virtuales (VM) justo a tiempo (JIT) de Microsoft Defender para la nube. Esto reduce la exposición a los ataques al tiempo que proporciona un fácil acceso cuando necesita conectarse a una máquina virtual.

Para obtener una explicación completa sobre cómo funciona JIT y la lógica subyacente, consulte [Just-in-time explicado](#) .

Para obtener una explicación completa de los requisitos de privilegios, consulte [¿Qué permisos se necesitan para configurar y usar JIT?](#) .

Esta página le enseña cómo incluir JIT en su programa de seguridad. Aprenderá a:

- **Habilite JIT en sus máquinas virtuales** : puede habilitar JIT con sus propias opciones personalizadas para una o más máquinas virtuales mediante Defender para la nube, PowerShell o la API de REST. Como alternativa, puede habilitar JIT con parámetros predeterminados codificados de forma rígida desde máquinas virtuales de Azure. Cuando está habilitado, JIT bloquea el tráfico entrante a sus máquinas virtuales de Azure y AWS mediante la creación de una regla en su grupo de seguridad de red.
- **Solicite acceso a una VM que tenga JIT habilitado** : el objetivo de JIT es garantizar que, aunque su tráfico entrante esté bloqueado, Defender for Cloud aún brinde acceso fácil para conectarse a las VM cuando sea necesario. Puede solicitar acceso a una máquina virtual habilitada para JIT desde Defender para la nube, máquinas virtuales de Azure, PowerShell o la API de REST.
- **Audite la actividad** : para asegurarse de que sus máquinas virtuales estén protegidas adecuadamente, revise los accesos a sus máquinas virtuales habilitadas para JIT como parte de sus controles de seguridad regulares.

Disponibilidad

Aspecto	Detalles
Estado de lanzamiento:	Disponibilidad general (GA)
Máquinas virtuales compatibles:	<ul style="list-style-type: none">✓ Máquinas virtuales implementadas a través de Azure Resource Manager.✗ Máquinas virtuales implementadas con modelos de implementación clásicos. Obtenga más información sobre estos modelos de implementación .✗ Máquinas virtuales protegidas por Azure Firewalls ¹ controladas por Azure Firewall Manager .✓ Instancias de AWS EC2 (versión preliminar)
Roles y permisos requeridos:	<p>Los roles Reader y SecurityReader pueden ver el estado y los parámetros de JIT.</p> <p>Para crear funciones personalizadas que puedan funcionar con JIT, consulte ¿Qué permisos se necesitan para configurar y usar JIT? .</p> <p>Para crear un rol con privilegios mínimos para los usuarios que necesitan solicitar acceso JIT a una VM y no realizar otras operaciones JIT, use el script Set-JitLeastPrivilegedRole de las páginas de la comunidad de Defender for Cloud GitHub.</p>
Nubes:	<ul style="list-style-type: none">✓ Nubes comerciales✓ Nacional (Azure Government, Azure China 21Vianet)✓ Cuentas de AWS conectadas (versión preliminar)

¹ para cualquier VM protegida por Azure Firewall, JIT solo protegerá completamente la máquina si está en la misma VNET que el firewall. Las máquinas virtuales que utilizan emparejamiento de VNET no estarán completamente protegidas.

Habilitar el acceso a máquinas virtuales JIT

Puede habilitar el acceso a máquinas virtuales JIT con sus propias opciones personalizadas para una o más máquinas virtuales mediante Defender for Cloud o mediante programación.

Como alternativa, puede habilitar JIT con parámetros predeterminados codificados de forma rígida desde máquinas virtuales de Azure.

Cada una de estas opciones se explica en una pestaña separada a continuación.

Para habilitar el acceso justo a tiempo a la máquina virtual desde PowerShell, use el cmdlet oficial de Microsoft Defender para Cloud PowerShell Set-AzJitNetworkAccessPolicy.

Ejemplo: habilite el acceso a máquinas virtuales justo a tiempo en una máquina virtual específica con las siguientes reglas:

- Cerrar los puertos 22 y 3389
- Establezca una ventana de tiempo máxima de 3 horas para cada uno para que puedan abrirse por solicitud aprobada
- Permita que el usuario que solicita acceso controle las direcciones IP de origen
- Permitir que el usuario que solicita acceso establezca una sesión exitosa tras una solicitud de acceso justo a tiempo aprobada

Los siguientes comandos de PowerShell crean esta configuración JIT:

1. Asigne una variable que contenga las reglas de acceso a máquinas virtuales justo a tiempo para una máquina virtual:

```
$jitpolicy = (@{  
  
id="/subscriptions/subscriptionid/resourcegroups/resourcegroup/providers/microsof  
t.compute/virtualmachines/vmname";  
  ports=(@{  
    number=22;  
    protocol="*";  
    allowedsourceaddressprefix=@("*");  
    maxrequestaccessduration="pt3h"},  
    @{  
      number=3389;  
      protocol="*";  
      allowedsourceaddressprefix=@("*");  
      maxrequestaccessduration="pt3h"}}))
```

Inserte las reglas de acceso a la máquina virtual justo a tiempo en una matriz

```
$JitPolicyArr=@($JitPolicy)
```

Configure las reglas de acceso a la máquina virtual justo a tiempo en la máquina virtual seleccionada:

```
Set-AzJitNetworkAccessPolicy -Kind "Basic" -Location "LOCATION" -Name "default" -  
ResourceGroupName "RESOURCEGROUP" -VirtualMachine $JitPolicyArr|
```

Utilice el parámetro -Name para especificar una máquina virtual. Por ejemplo, para establecer la configuración JIT para dos máquinas virtuales diferentes, VM1 y VM2, use: Set-AzJitNetworkAccessPolicy -Name VM1 y Set-AzJitNetworkAccessPolicy -Name VM2.

Solicitar acceso a una máquina virtual habilitada para JIT

Puede solicitar acceso a una máquina virtual habilitada para JIT desde Azure Portal (en Defender para la nube o máquinas virtuales de Azure) o mediante programación.

Cada una de estas opciones se explica en una pestaña separada a continuación.

En el siguiente ejemplo, puede ver una solicitud de acceso de máquina virtual justo a tiempo a una máquina virtual específica en la que se solicita que se abra el puerto 22 para una dirección IP específica y durante un período de tiempo específico:

Ejecute lo siguiente en PowerShell:

1. Configure las propiedades de acceso a la solicitud de VM:

```
$JitPolicyVm1 = (@{  
id="/subscriptions/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/VMNAME";  
  ports=@(  
    number=22;  
    endTimeUtc="2022-08-16T17:00:00.3658798Z";  
    allowedSourceAddressPrefix=@("192.168.100.89")})})
```

Inserte los parámetros de solicitud de acceso a la máquina virtual en una matriz:

```
$JitPolicyArr=@($JitPolicyVm1)
```

Envíe la solicitud de acceso (utilice el ID de recurso del paso 1)

```
Start-AzJitNetworkAccessPolicy -ResourceId  
"/subscriptions/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Security  
/locations/LOCATION/jitNetworkAccessPolicies/default" -VirtualMachine $JitPolicyArr
```

Auditar la actividad de acceso JIT en Defender for Cloud

Puede obtener información sobre las actividades de las máquinas virtuales mediante la búsqueda de registros. Para ver los registros:

1. En **Acceso a máquina virtual justo a tiempo**, seleccione la pestaña **Configurado**.
2. Para la máquina virtual que desea auditar, abra el menú de puntos suspensivos al final de la fila.

3. Seleccione **Registro** de actividad en el menú.

Microsoft Defender for Cloud | Just in time VM access

Showing subscription 'Ben Kliger'

Virtual machines

Configured Not Configured Unsupported

VMs for which the just in time VM access control is already in place. Presented data is for the last week.

22 VMs

Request access

Search to filter items...

Virtual machine	Approved	Last access	Connection details	Last user
VMTEST	1 Requests	7/8/20, 2:58 PM	Ports: 3389	
testing321	0 Requests	N/A	-	
PE-vm	0 Requests	N/A	-	
VM1	1 Requests	7/8/20, 2:52 PM	Ports: 22	
testing3	0 Requests	N/A	-	

Activity Log

El registro de actividad proporciona una vista filtrada de las operaciones anteriores de esa máquina virtual junto con la hora, la fecha y la suscripción.

4. Para descargar la información de registro, seleccione **Descargar como CSV**.

Como funciona

Lo que realmente hace la función de JIT es automatizar la excepción del grupo de seguridad de red NSG para permitirme conectarme de manera predeterminada la VM esta bloqueada y esta bloqueando cualquier administración remota de rdp o ssh lo que se hace es ir al portal de Azure luego al centro de seguridad y habilitar el JIT para esa maquina

Virtual machines

Configured Recommended No recommendation

VMs for which we recommend you to apply the just in time VM access control.

2 VMs

Enable JIT on 1 VMs

Search to filter items...

VIRTUAL MACHINE	STATE	SEVERITY
ASC-JIT-VM	Open	High
VM	Open	High

Luego se especifica el tiempo que se tendrá acceso

JIT VM access configuration
ASC-JIT-VM

+ Add Save X Discard

Configure the ports for which the just in time VM access will be applicable

PORT	PROT...	ALLOWED SOU...	IP RANGE	TIME RANGE (H...	
22 (Recommended)	Any	Per request	N/A	3 hours	...
3389 (Recommended)	Any	Per request	N/A	3 hours	...
5985 (Recommended)	Any	Per request	N/A	3 hours	...
5986 (Recommended)	Any	Per request	N/A	3 hours	...

Add port configuration

* Port
3389

Protocol
☒ Any ☐ TCP ☐ UDP

Allowed source IPs
☒ Per request ☐ CIDR block

IP addresses ⓘ

Max request time
 3 (hours)

Discard OK

Cuando necesito acceder a mi maquina virtual vuelvo al portal de azure luego voy al centro de seguridad y solicito el acceso para esa maquina en este punto determina cual es mi dirección ip publica e ira y modificara el grupo de seguridad de la red para permitir una excepción para cualquier protocolo ya sea RDP , SSH, WS y agregara esa excepción solo para mi ip después cuando termine el tiempo se volverá a cerrar

Virtual machines

Configured Recommended No recommendation

VMs for which the just in time VM access control is already in place. Presented data is for the last week.

1 VMs

Search to filter items...

	VIRTUAL MACHINE	APPROVED	LAST ACCESS	LAST USER	
<input checked="" type="checkbox"/>	ASC-JIT-VM	0 Requests	N/A	N/A	...

Request access