Lanzamientos y actualizaciones

Lanzamientos de software, guía de actualización, notificaciones de mantenimiento y garantía de calidad.

¿Cuál es el programa de garantía de calidad de Cyber Crucible?

Cyber Crucible se somete a numerosas etapas de pruebas internas, así como a validación externa, incluidas las pruebas del Microsoft Windows Hardware Certification Program, para garantizar su funcionalidad en todos los sistemas operativos de Microsoft, incluso hasta Server 2008 R2.

Esto puede verse al navegar por el Windows Server Catalog, que muestra únicamente los controladores que han superado la validación WHCP. Así como buscando en la lista Microsoft Altitude, que muestra la altitud de todos los controladores registrados.

- https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/allocated-altitudes
- Windows Server Catalog - Cyber Crucible

69369886.png

06 de marzo de 2024

Resumen del problema

Una interrupción de red ocurrida el 6MAR2024 afectó el acceso frontal al panel de control de Cyber Crucible
y el acceso a la telemetría a través de la API. Este problema se ha resuelto desde el 7MAR2024.

Causa raíz

A las 0400 UTC del 6MAR2024, el tráfico de telemetría comenzó a aumentar hasta alcanzar eventualmente el 1600% del tráfico
normal de agentes. Además, el ancho de banda de red entre las instancias de AWS comenzó a limitarse a
velocidades reducidas entre los balanceadores de carga, servidores y bases de datos alojados en AWS. En
múltiples zonas, las restricciones de ancho de banda fueron variables y oscilaron entre una pérdida total de transmisión (0% de capacidad) hasta el 50% de la capacidad. La disponibilidad del DNS de AWS también se vio comprometida.
Se confirmó que el tráfico de red entrante hacia Cyber Crucible era tráfico válido de agentes de clientes
existentes. El tráfico de bots hacia los balanceadores de carga no aumentó en volumen.
El ancho de banda adicional no fue el factor principal de la indisponibilidad de los servidores, pero exacerbó
los problemas de ancho de banda del middleware y la base de datos.
El aumento en el tráfico de agentes durante ese período ha disminuido parcialmente.
En este momento, Cyber Crucible comunica que no existe correlación entre las interrupciones de nube publicadas el
6MAR2024 y los problemas de AWS o el aumento del tráfico.

Impacto

El acceso al panel de control y a las API de Cyber Crucible se habría visto retrasado o no disponible. La telemetría de los agentes instalados se preservó por completo, y pudo haber sufrido retrasos en su envío
a la base de datos, pero no se perdió ninguna telemetría. Las protecciones de los agentes en los endpoints no se vieron
afectadas en absoluto, funcionando con normalidad, ya que ningún análisis o protección depende de la conexión de red con
ninguna API externa. En este momento, toda la telemetría se ha “puesto al día” en el panel de control.

Resolución

Cyber Crucible creó múltiples servidores dentro y fuera de AWS. La estabilidad de la red dentro de AWS parece haber mejorado durante la noche (7MAR2024), observándose mejoras ya desde las 0200 UTC. Cyber Crucible está operando actualmente al 500% de la capacidad de los servidores, calculado en función del
ancho de banda de tráfico máximo, el cual ha disminuido. El equipo ha estado reemplazando los servidores alojados en AWS a medida que estos pierden conectividad de red.

Para ser claros, el escalado adicional de servidores no fue una solución eficaz en este caso. Cyber Crucible ha comenzado la transición para dejar de utilizar AWS como único proveedor de alojamiento en la nube.
El trabajo para lograr independencia de plataforma en la nube ya llevaba meses en curso, con planes iniciales
de dejar de depender exclusivamente de AWS en el segundo trimestre de 2024. Las pruebas de extremo a extremo, incluidos todos los

esquemas necesarios de doble cifrado y autenticación x509 para nuestros diversos servidores y servicios, se completaron a finales de febrero de 2024. Los problemas de red que experimentamos con AWS han acelerado la transición, originalmente planificada para el segundo trimestre, adelantándola un mes
respecto al cronograma.

¿Cómo puedo gestionar las estrategias de actualización para grupos y agentes?

Gestionar la configuración de actualización de grupo

Los grupos tienen la actualización automática habilitada de forma predeterminada y los agentes siguen la configuración de actualización de su grupo de forma predeterminada. La configuración de actualización de grupo se puede ver en la página de Grupos:

85295158.png?width=680
La primera columna muestra si el grupo tiene la actualización automática activada o desactivada. La segunda columna muestra qué versión está aprobada para las actualizaciones de los agentes en este grupo que no están anulando la configuración de actualización de su grupo.

Cuando los grupos tienen la actualización automática activada, la columna de versión de agente aprobada mostrará la última versión de agente publicada y no se puede editar.

Cuando los grupos tienen la actualización automática desactivada, la columna de versión de agente aprobada se puede editar haciendo doble clic en la celda y seleccionando la versión que desea aprobar. También existe la opción de desactivar completamente la actualización (la opción "No Actualizar"). Tenga en cuenta que los agentes no revertirán a versiones anteriores.

Tenga en cuenta que la configuración de actualización de grupo se aplica al instalar un agente para decidir con qué versión se debe instalar el agente. Si el grupo tiene la actualización automática desactivada y "No Actualizar" seleccionado, entonces el agente se instalará de forma predeterminada con la última versión de agente disponible.

Gestionar la configuración de actualización de agentes

Los agentes seguirán la configuración de actualización de su grupo de forma predeterminada, pero los agentes pueden configurarse para anular la configuración de actualización de su grupo y seguir la suya propia. La configuración de actualización de agentes se puede ver en la página de Agentes:

85131315.png?width=680
Cuando un agente está anulando la configuración de actualización de su grupo, las columnas de actualización automática y versión de agente aprobada son editables, donde los usuarios pueden configurar la configuración de actualización del agente para seguir en lugar de seguir la configuración de actualización del grupo.

Cuando un agente está siguiendo la configuración de actualización de su grupo, las columnas de actualización automática y versión de agente aprobada no son editables y mostrarán la configuración de actualización del grupo.

¿Qué significa "Actualización preparada"?

Actualizar Cyber Crucible es un proceso automatizado, protegido y de varios pasos.

La actualización requiere un reinicio para surtir efecto, una vez que se ha obtenido de los servidores de Cyber Crucible.

Version	Attention
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)

Si bien algunas actualizaciones requieren varios pasos desde versiones muy antiguas, las actualizaciones pueden omitir varias versiones si es necesario.

Por ejemplo, las siguientes máquinas descargaron la versión 4.4.0.6, pero no se reiniciaron antes de que se lanzara la versión 4.4.0.7.

Ahora tendrán la versión 4.4.0.7 en ejecución cuando se reinicien.

Version	Attention
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)

En más detalle, actualizar Cyber Crucible requiere los siguientes pasos:

1. El software de Cyber Crucible recibe un aviso de que hay una actualización disponible.
2. Este aviso de actualización está firmado con RSA, para garantizar que un atacante no pueda forzar una actualización maliciosa. Se verifica que este aviso de actualización sea auténtico. Esto forma parte del diseño de producto de confianza cero (zero trust) de Cyber Crucible.
3. El agente descarga la actualización.
4. La actualización se valida para garantizar que no haya sido corrompida ni manipulada de ninguna otra forma.
5. La actualización prepara el nuevo software para su instalación. Los mecanismos de protección de Cyber Crucible en memoria y en disco impiden que se actualice o que el software sea reemplazado, excepto durante el arranque.
6. Se envía una notificación a los servidores de Cyber Crucible indicando que la actualización está lista y correctamente posicionada, tras la verificación.
7. Al reiniciarse, la actualización se aplica al software, y el software de Cyber Crucible responde con la nueva versión. El aviso de "Actualización preparada" desaparece.

¿Cyber Crucible requiere un reinicio para actualizarse?

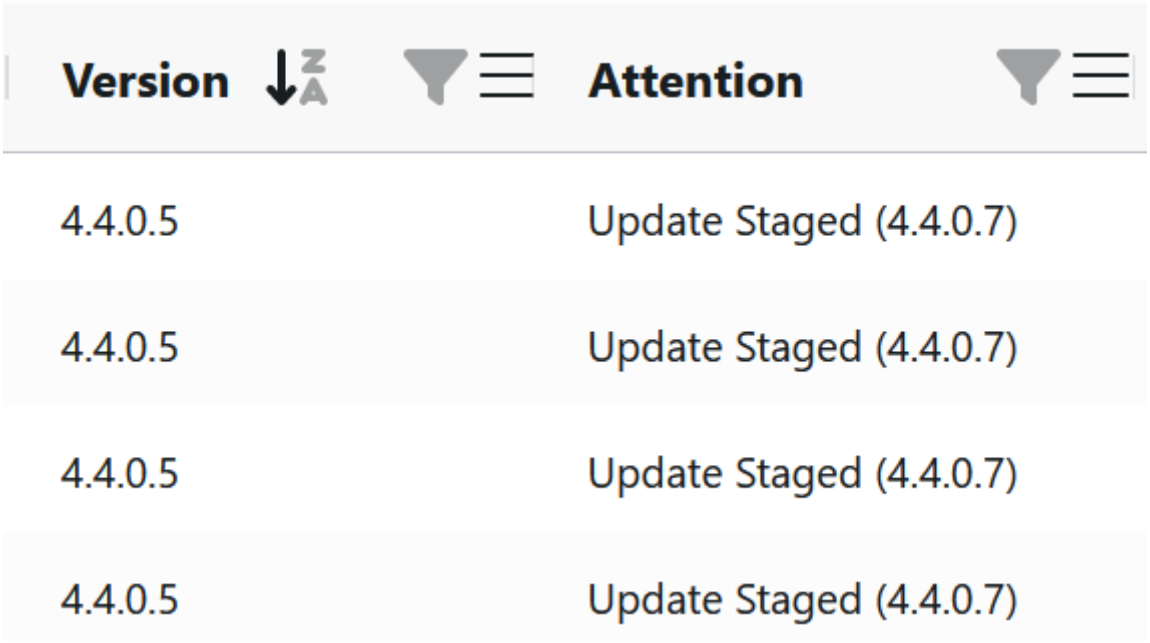
Sí, existen diversas protecciones de memoria, del sistema de archivos y del sistema operativo que el software de Cyber Crucible utiliza para protegerse contra intentos de manipulación o degradación de su rendimiento por parte de atacantes.

Esto forma parte del diseño de producto de confianza cero (zero trust) que utiliza Cyber Crucible.

La actualización requiere reemplazar el controlador y los servicios.

Al reiniciar, se crea una ventana en la que el software de Cyber Crucible permite que se produzca una actualización correctamente verificada.

Una actualización está lista para el reinicio cuando se observa lo siguiente en la página de Administrar Agentes.



Version	Attention
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)

¿Cyber Crucible actualizará varias versiones a la vez?

Si bien la actualización de varias versiones rara vez puede necesitar múltiples actualizaciones, normalmente las actualizaciones se realizan todas de una sola vez, incluso si un agente tiene varias versiones de atraso respecto a la más reciente.

Por ejemplo, los agentes que se muestran a continuación primero descargaron la versión 4.4.0.6 para actualizarse. No se reiniciaron para aplicar la actualización antes de que se publicara la versión 4.4.0.7. Cuando se publicó la versión 4.4.0.7, los agentes descargaron y prepararon (staged) la 4.4.0.7.

Cuando los sistemas se reinicien, se estará ejecutando Cyber Crucible 4.4.0.7, y el mensaje de Actualización Preparada (Staged Update) desaparecerá.

Version	Attention
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)

¿Cuál es su estrategia de actualización de software?

El software de Cyber Crucible no depende de flujos continuos de actualizaciones de firmas, tratando de alcanzar a los atacantes.

Aproximadamente una vez al mes, se publican nuevas funciones, mejoras en la metodología de confianza cero y mejoras en el módulo de análisis de comportamiento.

Todas las versiones de software publicadas por Cyber Crucible también son probadas, aprobadas y certificadas por el Microsoft Hardware Compatibility Program después de pasar nuestras propias pruebas rigurosas.

La actualización requiere un reinicio antes de que surta efecto.

Gestionar la configuración de actualización de grupos

Los grupos tienen la actualización automática habilitada de forma predeterminada y los agentes siguen la configuración de actualización de su grupo de forma predeterminada. La configuración de actualización de grupos se puede ver en la página Groups:

85426272.png?width=680
La primera columna muestra si el grupo tiene la actualización automática activada o desactivada. La segunda columna muestra qué versión está aprobada para las actualizaciones de los agentes de este grupo que no anulan la configuración de actualización de su grupo.

Cuando los grupos tienen la actualización automática activada, la columna de versión de agente aprobada mostrará la última versión de agente publicada y no será editable.

Cuando los grupos tienen la actualización automática desactivada, la columna de versión de agente aprobada es editable haciendo doble clic en la celda y seleccionando la versión que desea aprobar. También existe la opción de desactivar por completo las actualizaciones (la opción “Do Not Update”). Tenga en cuenta que los agentes no revertirán a versiones anteriores.

Tenga en cuenta que la configuración de actualización de grupos se aplica al instalar un agente para decidir con qué versión debe instalarse el agente. Si el grupo tiene la actualización automática desactivada y se ha seleccionado “Do Not Update”, el agente se instalará por defecto

con la última versión de agente disponible.

Gestionar la configuración de actualización de agentes

Los agentes seguirán la configuración de actualización de su grupo de forma predeterminada, pero pueden configurarse para anular la configuración de actualización de su grupo y seguir la suya propia. La configuración de actualización de agentes se puede ver en la página Agents:

85557298.png?width=680
Cuando un agente está anulando la configuración de actualización de su grupo, las columnas de actualización automática y de versión de agente aprobada son editables, de modo que los usuarios pueden configurar la actualización del agente para que este la siga en lugar de seguir la configuración del grupo.

Cuando un agente sigue la configuración de actualización de su grupo, las columnas de actualización automática y de versión de agente aprobada no son editables y mostrarán la configuración de actualización del grupo.