Lançamentos e Atualizações

Lançamentos de software, orientações de atualização, notificações de manutenção e garantia de qualidade.

- Qual é o programa de garantia de qualidade da Cyber Crucible?
- 06 de março de 2024
- Como posso gerenciar estratégias de atualização para grupos e agentes?
- O que significa "Atualização Preparada"?
- O Cyber Crucible exige uma reinicialização para atualizar?
- A Cyber Crucible atualizará várias versões de uma só vez?
- Qual é a sua estratégia de atualização de software?

Qual é o programa de garantia de qualidade da Cyber Crucible?

A Cyber Crucible passa por muitos estágios de testes internos, bem como validação externa, incluindo os testes do Microsoft Windows Hardware Certification Program, para garantir a funcionalidade em todos os Sistemas Operacionais Microsoft, remontando até o Server 2008 R2.

Isso pode ser verificado navegando pelo Windows Server Catalog, que mostra apenas os drivers que passaram pela validação WHCP. Assim como pesquisando na lista Microsoft Altitude, que mostra a altitude de todos os drivers registrados.

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

69369886.png

06 de março de 2024

Resumo do Problema

Uma interrupção de rede ocorrida em 06/03/2024 afetou o acesso front-end ao painel do Cyber Crucible
e o acesso à telemetria via API. Este problema foi resolvido em 07/03/2024.

Causa Raiz

Às 04h00 UTC de 06/03/2024, o tráfego de telemetria começou a aumentar até atingir eventualmente 1600% do tráfego
normal de agentes. Além disso, a largura de banda da rede entre as instâncias da AWS começou a ser limitada a
velocidades reduzidas entre os balanceadores de carga, servidores e bancos de dados hospedados na AWS. Em
múltiplas zonas, as restrições de largura de banda foram variáveis e variaram de perda total de transmissão
(0% da capacidade) a 50% da capacidade. A disponibilidade do DNS da AWS também foi comprometida.
Confirmou-se que o tráfego de rede recebido pelo Cyber Crucible era tráfego válido de agentes de clientes
existentes. O tráfego de bots para os balanceadores de carga não aumentou em volume.
A largura de banda adicional não foi o principal fator para a indisponibilidade dos servidores, mas agravou
os problemas de largura de banda do middleware e do banco de dados.
O pico no tráfego de agentes durante esse período diminuiu parcialmente.
Neste momento, o Cyber Crucible não observa nenhuma correlação entre as interrupções de nuvem divulgadas em
06/03/2024 e os problemas da AWS ou o pico de tráfego.

Impacto

O acesso ao painel e às APIs do Cyber Crucible pode ter sido atrasado ou indisponível.
A telemetria dos agentes instalados foi totalmente preservada, podendo ter havido atraso no envio ao banco de dados, mas nenhuma telemetria foi perdida. As proteções dos endpoints dos agentes permaneceram
completamente inalteradas, funcionando normalmente, pois nenhuma análise ou proteção depende de conexão de rede com
quaisquer APIs upstream. Neste momento, toda a telemetria já foi atualizada no painel.

Resolução

O Cyber Crucible criou múltiplos servidores dentro e fora da AWS. A estabilidade da rede dentro da AWS parece ter melhorado durante a noite (07/03/2024), com melhorias observadas já a partir das 02h00 UTC. O Cyber Crucible está atualmente operando a 500% da capacidade dos servidores, calculada com base
na largura de banda de tráfego de pico, que já diminuiu. A equipe tem substituído os servidores hospedados na
AWS à medida que perdem a conectividade de rede.

Para deixar claro, o aumento adicional de escala dos servidores não foi uma resolução eficaz nesta questão.
O Cyber Crucible começou a transição do uso da AWS como único provedor de hospedagem em nuvem. O trabalho
para viabilizar a agnosticismo em relação à plataforma de nuvem já vinha sendo desenvolvido há meses, com planos
iniciais de deixar de usar a AWS como único provedor no segundo trimestre de 2024. Os testes de ponta a ponta, incluindo todos os

esquemas necessários de dupla criptografia e autenticação x509 para nossos diversos servidores e serviços, foram concluídos no final de fevereiro de 2024. Os problemas de rede que enfrentamos com a AWS aceleraram a transição, originalmente planejada para o segundo trimestre, fazendo-a começar um mês antes
do previsto.

Como posso gerenciar estratégias de atualização para grupos e agentes?

- Gerenciar Configurações de Atualização de Grupo
- Gerenciar Configurações de Atualização de Agente

Gerenciar Configurações de Atualização de Grupo

Os grupos têm a atualização automática ativada por padrão, e os agentes seguem as configurações de atualização do seu grupo por padrão. As configurações de atualização de grupo podem ser visualizadas na página Grupos:

85295158.png?width=680
A primeira coluna mostra se o grupo tem a atualização automática ativada ou desativada. A segunda coluna mostra qual versão está aprovada para atualizações dos agentes deste grupo que não estão substituindo as configurações de atualização do grupo.

Quando os grupos têm a atualização automática ativada, a coluna de versão de agente aprovada mostrará a versão de agente mais recente lançada e não será editável.

Quando os grupos têm a atualização automática desativada, a coluna de versão de agente aprovada é editável ao clicar duas vezes na célula e selecionar a versão que deseja aprovar. Também há uma opção para desativar completamente as atualizações (a opção “Não Atualizar”). Observe que os agentes não farão downgrade de versões.

Observe que as configurações de atualização de grupo são aplicadas ao instalar um agente para decidir com qual versão o agente deve ser instalado. Se o grupo tiver a atualização automática desativada e a opção “Não Atualizar” selecionada, então o agente será instalado por padrão com a versão de agente disponível mais recente.

Gerenciar Configurações de Atualização de Agente

Os agentes seguirão as configurações de atualização do seu grupo por padrão, mas os agentes podem ser configurados para substituir as configurações de atualização do grupo e seguir as suas próprias. As configurações de atualização de Agente podem ser visualizadas na página Agentes:

85131315.png?width=680
Quando um agente está substituindo as configurações de atualização do seu grupo, as colunas de atualização automática e de versão de agente aprovada são editáveis, onde os usuários podem configurar as configurações de atualização do agente a serem seguidas em vez de seguir as configurações de atualização do grupo.

Quando um agente está seguindo as configurações de atualização do seu grupo, as colunas de atualização automática e de versão de agente aprovada não são editáveis e mostrarão as configurações de atualização do grupo.

O que significa "Atualização Preparada"?

Atualizar o Cyber Crucible é um processo automatizado, protegido e realizado em várias etapas.

A atualização requer uma reinicialização para entrar em vigor, após ser obtida dos servidores da 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)

Embora algumas atualizações exijam várias etapas a partir de versões muito antigas, as atualizações podem pular várias versões, se necessário.

Por exemplo, as máquinas abaixo baixaram a versão 4.4.0.6, mas não foram reiniciadas antes do lançamento da versão 4.4.0.7.

Elas agora executarão a versão 4.4.0.7 quando forem reiniciadas.

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)

Em mais detalhes, a atualização do Cyber Crucible requer as seguintes etapas:

1. O software Cyber Crucible recebe um aviso de que uma atualização está disponível.
2. Este aviso de atualização é assinado digitalmente com RSA, para garantir que um invasor não possa forçar uma atualização maliciosa. Este aviso de atualização é verificado quanto à sua autenticidade. Isso faz parte do design de produto de confiança zero (zero trust) da Cyber Crucible.
3. A atualização é baixada pelo agente.
4. A atualização é validada, para garantir que não tenha sido corrompida ou adulterada de qualquer forma.
5. A atualização prepara o novo software para instalação. Os mecanismos de proteção do Cyber Crucible, tanto na memória quanto no disco, impedem que ele seja atualizado ou que o software seja substituído, exceto durante a inicialização (boot).
6. Uma notificação é enviada aos servidores da Cyber Crucible informando que a atualização está pronta e devidamente posicionada, após a verificação.
7. Após a reinicialização, a atualização é aplicada ao software, e o software Cyber Crucible responde com a nova versão. O aviso de "Atualização Preparada" desaparece.

O Cyber Crucible exige uma reinicialização para atualizar?

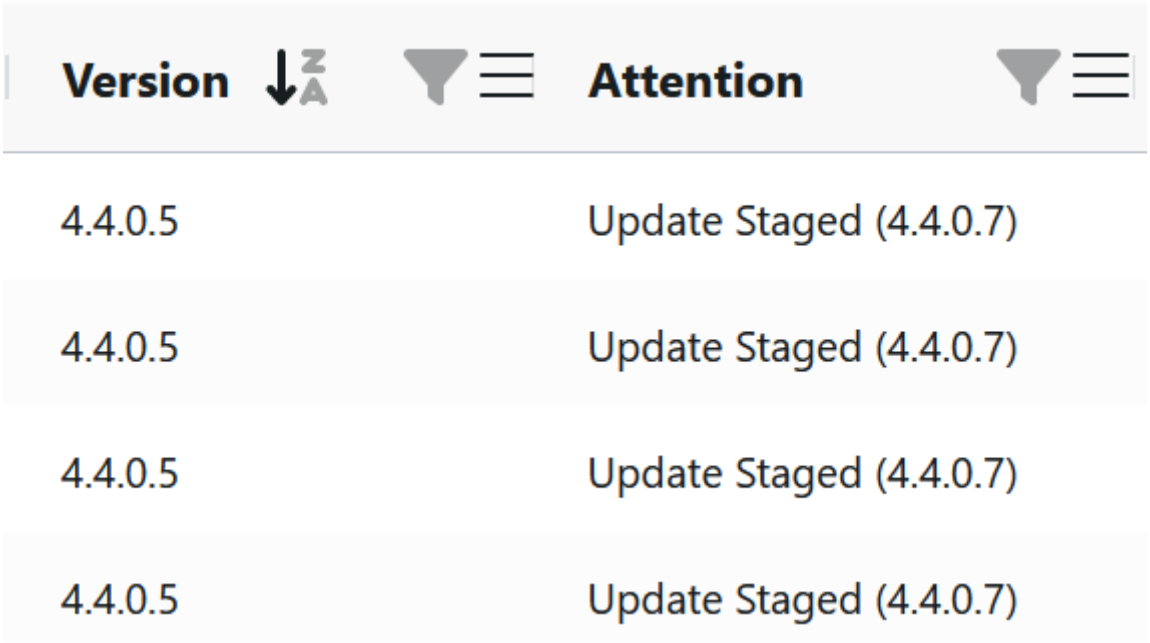
Sim, existem diversas proteções de memória, sistema de arquivos e sistema operacional que o software Cyber Crucible utiliza para se proteger contra tentativas de invasores de adulterar ou degradar seu desempenho.

Isso faz parte do design de produto de confiança zero (zero trust) do Cyber Crucible em uso.

A atualização exige a substituição do driver e dos serviços.

Uma janela é criada após a reinicialização, na qual o software Cyber Crucible permite que uma atualização devidamente verificada seja realizada.

Uma atualização está pronta para reinicialização quando o seguinte é observado na página Manage Agents.



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)

A Cyber Crucible atualizará várias versões de uma só vez?

Embora a atualização de várias versões raramente possa exigir múltiplas atualizações, as atualizações normalmente são feitas de uma só vez, mesmo que um agente esteja várias versões atrás da mais recente.

Por exemplo, os agentes vistos abaixo primeiro baixaram a versão 4.4.0.6 para atualizar. Eles não reiniciaram para aplicar a atualização antes do lançamento da versão 4.4.0.7. Quando a versão 4.4.0.7 foi lançada, os agentes baixaram e prepararam (staged) a versão 4.4.0.7.

Quando os sistemas reiniciarem, a Cyber Crucible 4.4.0.7 estará em execução, e a mensagem de Atualização 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)

Qual é a sua estratégia de atualização de software?

O software da Cyber Crucible não depende de fluxos contínuos de atualizações de assinaturas, tentando alcançar os atacantes.

Aproximadamente uma vez por mês, são lançados novos recursos, melhorias na metodologia de zero trust e melhorias no módulo de análise comportamental.

Todas as versões de software lançadas pela Cyber Crucible também são testadas, aprovadas e certificadas pelo Microsoft Hardware Compatibility Program após passarem pelos nossos próprios testes rigorosos.

A atualização requer uma reinicialização antes que a atualização entre em vigor.

Gerenciar Configurações de Atualização do Grupo

Os grupos têm a atualização automática ativada por padrão e os agentes seguem as configurações de atualização do seu grupo por padrão. As configurações de atualização do grupo podem ser visualizadas na página Grupos:

85426272.png?width=680
A primeira coluna mostra se o grupo tem a atualização automática ativada ou desativada. A segunda coluna mostra qual versão está aprovada para atualizações para os agentes deste grupo que não estão substituindo as configurações de atualização do grupo.

Quando os grupos têm a atualização automática ativada, a coluna de versão do agente aprovada mostrará a versão mais recente do agente lançada e não é editável.

Quando os grupos têm a atualização automática desativada, a coluna de versão do agente aprovada é editável ao clicar duas vezes na célula e selecionar qual versão você deseja aprovar. Também há uma opção para desativar completamente a atualização (a opção "Não Atualizar"). Observe que os agentes não farão downgrade de versões.

Observe que as configurações de atualização do grupo são aplicadas ao instalar um agente para decidir qual versão o agente deve instalar. Se o grupo tiver a atualização automática desativada e a opção "Não Atualizar" selecionada, então o agente instalará por padrão com a versão mais

recente disponível do agente.

Gerenciar Configurações de Atualização do Agente

Os agentes seguirão as configurações de atualização do seu grupo por padrão, mas os agentes podem ser configurados para substituir as configurações de atualização do grupo e seguir as suas próprias. As configurações de atualização do Agente podem ser visualizadas na página Agentes:

85557298.png?width=680
Quando um agente está substituindo as configurações de atualização do seu grupo, as colunas de atualização automática e versão do agente aprovada são editáveis, onde os usuários podem configurar as configurações de atualização do agente a seguir, em vez de seguir as configurações de atualização do grupo.

Quando um agente está seguindo as configurações de atualização do seu grupo, as colunas de atualização automática e versão do agente aprovada não são editáveis e mostrarão as configurações de atualização do grupo.