Versions et mises à jour

Versions logicielles, conseils de mise à niveau, notifications de maintenance et assurance qualité.

Qu'est-ce que le programme d'assurance qualité de Cyber Crucible ?

Cyber Crucible fait l'objet de nombreuses étapes de tests internes ainsi que de validations externes, notamment les tests du Microsoft Windows Hardware Certification Program, afin de garantir son bon fonctionnement sur tous les systèmes d'exploitation Microsoft, y compris ceux remontant à Server 2008 R2.

Cela peut être vérifié en parcourant le Windows Server Catalog, qui n'affiche que les pilotes ayant réussi la validation WHCP. Cela peut également être vérifié en recherchant dans la liste Microsoft Altitude, qui indique l'altitude de tous les pilotes enregistrés.

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

69369886.png

06 mars 2024

Résumé de l'incident

Une panne réseau survenue le 06/03/2024 a affecté l'accès à l'interface (front-end) du tableau de bord
Cyber Crucible ainsi que l'accès à la télémétrie via API. Ce problème a depuis été résolu au 07/03/2024.

Cause première

À 04h00 UTC le 06/03/2024, le trafic de télémétrie a commencé à augmenter progressivement pour atteindre finalement 1600 % du
trafic agent normal. De plus, la bande passante réseau entre les instances AWS a commencé à être limitée à
des débits réduits entre les équilibreurs de charge, serveurs et bases de données hébergés sur AWS. Sur
plusieurs zones, les contraintes de bande passante étaient variables et allaient d'une perte totale de transmission
(0 % de la capacité) à 50 % de la capacité. La disponibilité du DNS AWS a également été compromise.
Le trafic réseau entrant vers Cyber Crucible a été confirmé comme étant du trafic agent valide provenant de clients
existants. Le trafic de bots vers les équilibreurs de charge n'a pas augmenté en volume.
La bande passante supplémentaire n'était pas le principal facteur d'indisponibilité des serveurs, mais a aggravé
les problèmes de bande passante liés au middleware et aux bases de données.
Le pic de trafic agent observé durant cette période s'est partiellement résorbé.
À ce stade, Cyber Crucible ne communique sur aucune corrélation entre les pannes cloud publiées le
06/03/2024 et les problèmes AWS ou le pic de trafic.

Impact

L'accès au tableau de bord et aux API de Cyber Crucible aurait pu être retardé ou indisponible. La télémétrie provenant des agents installés a été entièrement préservée et sa transmission à la base de données a pu être retardée, mais aucune télémétrie n'a été perdue. Les protections des agents sur les postes n'ont été absolument pas affectées, fonctionnant normalement, car aucune analyse ni protection ne dépend d'une connexion réseau vers une quelconque API en amont. À ce stade, l'ensemble de la télémétrie a « rattrapé son retard » dans le tableau de bord.

Résolution

Cyber Crucible a créé plusieurs serveurs à l'intérieur et à l'extérieur d'AWS. La stabilité du réseau au sein d'AWS semble s'être améliorée durant la nuit (07/03/2024), avec des améliorations observées dès 02h00 UTC. Cyber Crucible fonctionne actuellement à 500 % de la capacité serveur, calculée sur la base de la bande passante de trafic de pointe qui s'est depuis résorbée. L'équipe a remplacé les serveurs hébergés sur AWS à mesure qu'ils perdaient leur connectivité réseau.

Pour être clair, l'ajout de capacité serveur supplémentaire n'a pas constitué une résolution efficace dans ce cas.
Cyber Crucible a entamé une transition visant à ne plus utiliser AWS comme unique fournisseur d'hébergement cloud.
Les travaux visant à assurer une indépendance vis-à-vis des plateformes cloud étaient déjà en cours depuis plusieurs mois, avec des plans initiaux de transition depuis AWS comme fournisseur unique prévus pour le T2 2024. Les tests de bout en bout, y compris tous les

schémas de double chiffrement et d'authentification x509 nécessaires pour nos différents serveurs et services, ont été achevés fin février 2024. Les problèmes réseau que nous avons rencontrés avec AWS ont accéléré cette transition, initialement prévue pour le T2, en la faisant débuter un mois avant la date prévue.

Comment puis-je gérer les stratégies de mise à jour pour les groupes et les agents ?

Gérer les paramètres de mise à jour des groupes

Les groupes ont la mise à jour automatique activée par défaut et les agents suivent les paramètres de mise à jour de leur groupe par défaut. Les paramètres de mise à jour des groupes peuvent être consultés sur la page Groupes :

85295158.png?width=680
La première colonne indique si la mise à jour automatique est activée ou désactivée pour le groupe. La deuxième colonne indique quelle version est approuvée pour les mises à jour des agents de ce groupe qui ne remplacent pas les paramètres de mise à jour de leur groupe.

Lorsque la mise à jour automatique est activée pour les groupes, la colonne de la version d'agent approuvée affiche la dernière version d'agent publiée et n'est pas modifiable.

Lorsque la mise à jour automatique est désactivée pour les groupes, la colonne de la version d'agent approuvée est modifiable en double-cliquant sur la cellule et en sélectionnant la version que vous souhaitez approuver. Il existe également une option permettant de désactiver complètement la mise à jour (l'option « Ne pas mettre à jour »). Notez que les agents ne rétrograderont pas de version.

Notez que les paramètres de mise à jour des groupes sont appliqués lors de l'installation d'un agent afin de déterminer avec quelle version l'agent doit être installé. Si le groupe a désactivé la mise à jour automatique et sélectionné « Ne pas mettre à jour », l'agent s'installera alors par défaut avec la dernière version d'agent disponible.

Gérer les paramètres de mise à jour des agents

Les agents suivent par défaut les paramètres de mise à jour de leur groupe, mais ils peuvent être configurés pour remplacer les paramètres de mise à jour de leur groupe par leurs propres paramètres. Les paramètres de mise à jour des agents peuvent être consultés sur la page Agents :

85131315.png?width=680
Lorsqu’un agent remplace les paramètres de mise à jour de son groupe, les colonnes de mise à jour automatique et de version d’agent approuvée sont modifiables, permettant aux utilisateurs de configurer les paramètres de mise à jour de l’agent qu’il devra suivre au lieu de suivre les paramètres de mise à jour du groupe.

Lorsqu’un agent suit les paramètres de mise à jour de son groupe, les colonnes de mise à jour automatique et de version d’agent approuvée ne sont pas modifiables et affichent les paramètres de mise à jour du groupe.

Que signifie « Mise à jour préparée » ?

La mise à jour de Cyber Crucible est un processus automatisé, protégé et comportant plusieurs étapes.

La mise à jour nécessite un redémarrage pour prendre effet, une fois récupérée depuis les serveurs 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)

Bien que certaines mises à jour nécessitent plusieurs étapes à partir de versions très anciennes, les mises à jour peuvent, si nécessaire, ignorer plusieurs versions.

Par exemple, les machines ci-dessous ont téléchargé la version 4.4.0.6, mais n'ont pas redémarré avant la publication de la version 4.4.0.7.

Elles exécuteront désormais la version 4.4.0.7 lors de leur redémarrage.

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)

Plus en détail, la mise à jour de Cyber Crucible nécessite les étapes suivantes :

1. Le logiciel Cyber Crucible reçoit une notification indiquant qu'une mise à jour est disponible.
2. Cette notification de mise à jour est signée RSA, afin de garantir qu'un attaquant ne puisse pas forcer une mise à jour malveillante. Cette notification de mise à jour est vérifiée comme étant authentique. Cela fait partie de la conception « zero trust » du produit Cyber Crucible.
3. La mise à jour est téléchargée par l'agent.
4. La mise à jour est validée, afin de s'assurer qu'elle n'a pas été corrompue ou altérée de quelque manière que ce soit.
5. La mise à jour prépare le nouveau logiciel en vue de son installation. Les mécanismes de protection de Cyber Crucible, en mémoire et sur disque, empêchent toute mise à niveau ou tout remplacement du logiciel, sauf pendant le démarrage.
6. Une notification est envoyée aux serveurs Cyber Crucible indiquant que la mise à jour est prête et correctement positionnée, après vérification.
7. Lors du redémarrage, la mise à jour est appliquée au logiciel, et le logiciel Cyber Crucible répond avec la nouvelle version. La notification « Mise à jour préparée » disparaît.

Cyber Crucible nécessite-t-il un redémarrage pour se mettre à jour ?

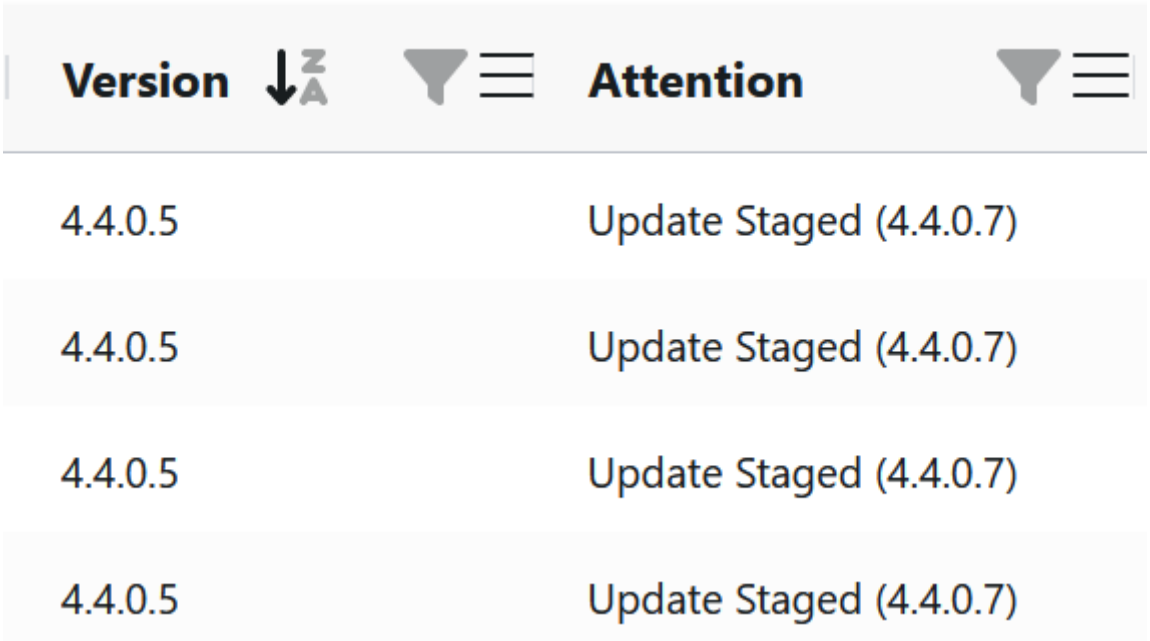
Oui, il existe diverses protections de la mémoire, du système de fichiers et du système d'exploitation que le logiciel Cyber Crucible exploite pour se protéger contre les tentatives d'altération ou de dégradation de ses performances par des attaquants.

Cela fait partie de la conception zero trust du produit Cyber Crucible en usage.

La mise à jour nécessite le remplacement du pilote et des services.

Une fenêtre est créée lors du redémarrage, au cours de laquelle le logiciel Cyber Crucible autorise l'application d'une mise à jour correctement vérifiée.

Une mise à jour est prête pour le redémarrage lorsque l'observation suivante apparaît sur la page Gérer les agents.

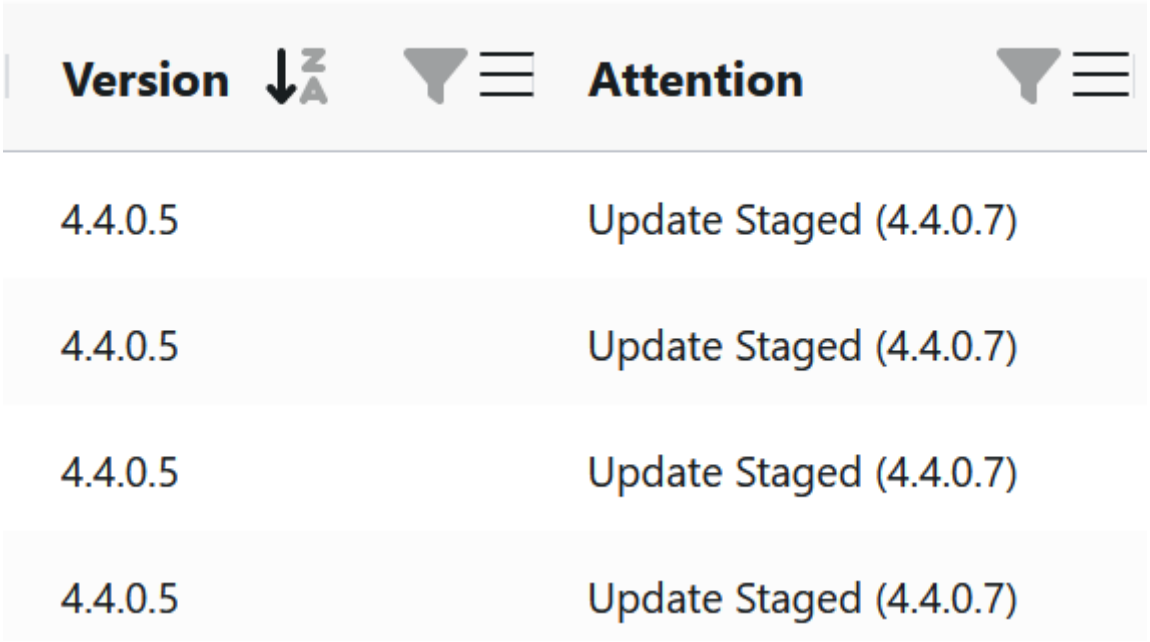


Cyber Crucible mettra-t-il à jour plusieurs versions en une seule fois ?

Bien que la mise à jour de plusieurs versions puisse rarement nécessiter plusieurs mises à jour, les mises à jour sont normalement effectuées en une seule fois, même si un agent a plusieurs versions de retard par rapport à la plus récente.

Par exemple, les agents présentés ci-dessous ont d'abord téléchargé la version 4.4.0.6 pour la mettre à jour. Ils n'ont pas redémarré pour appliquer la mise à jour avant la sortie de la version 4.4.0.7. Lorsque la version 4.4.0.7 est sortie, les agents ont téléchargé et préparé la version 4.4.0.7.

Lorsque les systèmes redémarrent, Cyber Crucible 4.4.0.7 sera en cours d'exécution, et le message de mise à jour préparée disparaîtra.



Quelle est votre stratégie de mise à jour logicielle ?

Le logiciel de Cyber Crucible ne repose pas sur des flux continus de mises à jour de signatures, tentant de rattraper les attaquants.

Environ une fois par mois, de nouvelles fonctionnalités, des améliorations de la méthodologie zero trust et des améliorations du module d'analyse comportementale sont publiées.

Toutes les versions logicielles publiées par Cyber Crucible sont également testées, approuvées et certifiées par le Microsoft Hardware Compatibility Program après avoir réussi nos propres tests rigoureux.

La mise à niveau nécessite un redémarrage avant qu'une mise à jour ne prenne effet.

Gérer les paramètres de mise à jour des groupes

Les groupes ont la mise à jour automatique activée par défaut et les agents suivent les paramètres de mise à jour de leur groupe par défaut. Les paramètres de mise à jour des groupes peuvent être consultés sur la page Groupes :

85426272.png?width=680
La première colonne indique si le groupe a la mise à jour automatique activée ou désactivée. La deuxième colonne indique quelle version est approuvée pour les mises à jour des agents de ce groupe qui ne remplacent pas les paramètres de mise à jour de leur groupe.

Lorsque les groupes ont la mise à jour automatique activée, la colonne de la version d'agent approuvée affiche la dernière version d'agent publiée et n'est pas modifiable.

Lorsque les groupes ont la mise à jour automatique désactivée, la colonne de la version d'agent approuvée est modifiable en double-cliquant sur la cellule et en sélectionnant la version que vous souhaitez approuver. Il existe également une option pour désactiver complètement la mise à jour (l'option « Ne pas mettre à jour »). Notez que les agents ne rétrograderont pas de version.

Notez que les paramètres de mise à jour du groupe sont appliqués lors de l'installation d'un agent pour déterminer avec quelle version l'agent doit s'installer. Si le groupe a la mise à jour automatique désactivée et que l'option « Ne pas mettre à jour » est sélectionnée, l'agent

s'installera alors par défaut avec la dernière version d'agent disponible.

Gérer les paramètres de mise à jour des agents

Les agents suivront par défaut les paramètres de mise à jour de leur groupe, mais les agents peuvent être configurés pour remplacer les paramètres de mise à jour de leur groupe afin de suivre les leurs. Les paramètres de mise à jour des agents peuvent être consultés sur la page Agents :

85557298.png?width=680
Lorsqu'un agent remplace les paramètres de mise à jour de son groupe, les colonnes de mise à jour automatique et de version d'agent approuvée sont modifiables et les utilisateurs peuvent configurer les paramètres de mise à jour de l'agent à suivre au lieu de suivre les paramètres de mise à jour du groupe.

Lorsqu'un agent suit les paramètres de mise à jour de son groupe, les colonnes de mise à jour automatique et de version d'agent approuvée ne sont pas modifiables et afficheront les paramètres de mise à jour du groupe.