Cisco Tetration Analytics

La plateforme Cisco Tetration Analytics[MC] permet d'effectuer efficacement les opérations de centre de données grâce à une visibilité omniprésente, à l'analyse des applications en fonction des comportements et à la migration vers un modèle de confiance zéro.

Présentation du produit

Les centres de données modernes sont dynamiques, la virtualisation étant compartimentée et les technologies de mobilité des charges de travail nécessitant un déploiement rapide des applications. De plus, les modèles de communication entre les composants des applications sont en constante évolution. En raison de ces progrès technologiques, 76 % du trafic des centres de données sont transversaux. En outre, les centres de données d'aujourd'hui exigent un réseau très disponible sans aucune interruption de service programmée. Cet environnement dynamique contribue à trois principaux défis :

- la visibilité omniprésente du trafic sur les infrastructures de centre de données et la conservation des données à long terme pour les analyses et investigations,
- la connaissance des communications et des dépendances pour toutes les applications dans le centre de données,
- la définition d'un modèle de politique de liste blanche, la détection d'écarts de comportement en temps réel et l'exécution des opérations d'investigation.

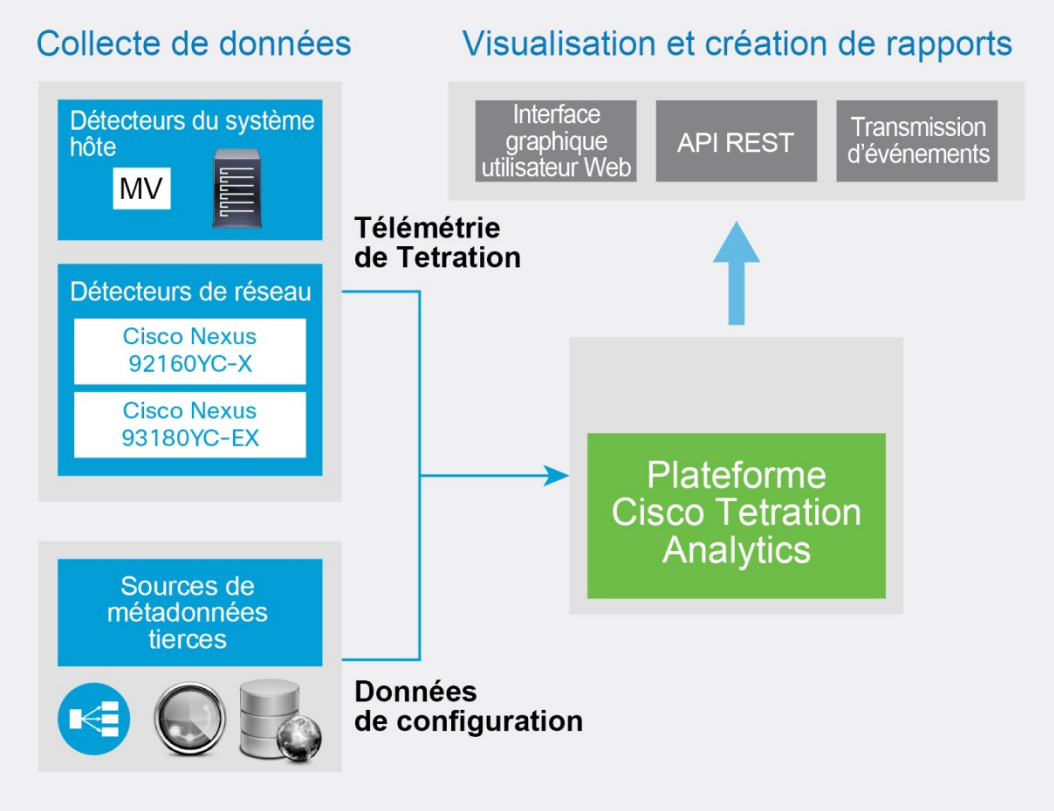
La nouvelle plateforme Cisco Tetration Analytics est conçue pour relever ces défis grâce à la collecte d'une télémétrie détaillée du trafic et à l'exécution d'analyses avancées par une approche algorithmique. Cette plateforme est conçue pour recueillir cette télémétrie détaillée à débit de ligne à l'échelle du centre de données. L'approche algorithmique comprend des techniques d'apprentissage automatique non surveillé et des analyses comportementales, afin d'offrir une solution clé en main. Cette solution est conçue pour atteindre les objectifs suivants :

- traiter des millions de flux par seconde, appliquer les algorithmes intelligents et fournir des analyses pratiques en quelques minutes,
- détecter et enregistrer des centaines de milliards d'enregistrements de télémétrie sans agrégation pour permettre une investigation à long terme,
- fournir une visibilité totale sur les composants des applications, leurs communications et leurs dépendances pour permettre la mise en œuvre du modèle de confiance zéro au sein du réseau.

La télémétrie détaillée de Cisco Tetration est recueillie grâce à des éléments appelés des détecteurs. La première version de la solution comprend deux types de détecteurs, les détecteurs de matériel et de logiciels (hôte). Grâce à ces deux types de détecteurs, cette solution est conçue pour prendre en charge des infrastructures de centre de donnée existantes (sur site) et de nouvelles infrastructures de centre de données (en terrain vierge).

La figure 1 illustre l'architecture de pointe de la plateforme Cisco Tetration Analytics.

Figure 1. Architecture de la plateforme Cisco Tetration Analytics



La plateforme Cisco Tetration Analytics possède trois couches principales de fonction :

- **Couche de collecte de données :** cette couche comprend principalement des détecteurs légers, qui sont les yeux et les oreilles de la plateforme d'analyse. Deux types de détecteurs sont utilisés :
  - des détecteurs de logiciels ou de système hôte : ils peuvent être installés sur tous les serveurs des terminaux des systèmes hôtes (virtualisés ou sans système d'exploitation),
  - des détecteurs de matériel : ils sont intégrés aux commutateurs Cisco Nexus[MD] de séries 92160YC-X, 93180YC-EX et 93108TC-EX.

  La télémétrie détaillée de Tetration collectée par ces détecteurs se compose de trois types de renseignements :
  - **Renseignements sur les flux :** ces renseignements contiennent des détails concernant les points d'extrémité, le protocole, les ports, l'heure de démarrage des flux, la durée de transmission des flux, etc.
  - **Variations entre paquets :** ces renseignements détectent les types de variation entre les paquets au sein des flux. Par exemple, les variations dans le TTL, les variations des indicateurs d'IP/TCP, la longueur des charges, etc.
  - **Détails du contexte :** les renseignements contextuels sont déterminés en dehors de l'en-tête de paquet. Dans le cas du détecteur de logiciels, ces renseignements comprennent les détails concernant le processus, le processus générant le flux, les identifiants de processus, l'utilisateur associé au processus, etc.

Les détecteurs ne traitent aucun renseignement sur les charges et aucun échantillonnage n'est exécuté. Les détecteurs sont conçus pour surveiller chaque paquet et chaque flux. En plus des détecteurs, cette couche comprend des sources de tierces parties, comme les équilibreurs de charge, les mises en correspondance de serveur DNS, etc. pour recueillir les renseignements de configuration. Ces données de configuration sont utilisées pour enrichir les renseignements fournis par la plateforme d'analyse.

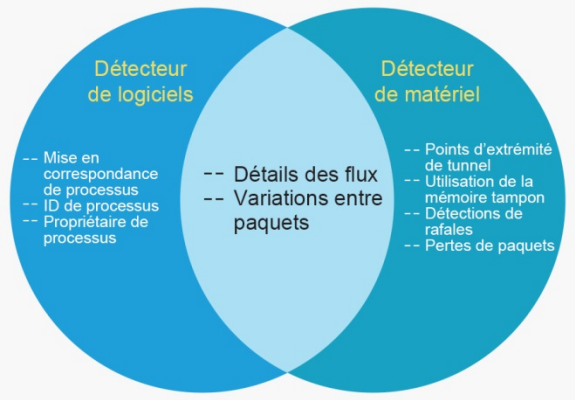
- **Couche d'analyse :** les données des détecteurs sont envoyées à la plateforme Cisco Tetration Analytics qui est le pivot de l'exécution des analyses. Cette plateforme de données volumineuses à plusieurs serveurs traite les renseignements de ces détecteurs et utilise l'apprentissage automatique sans supervision et l'apprentissage commandé, les analyses comportementales et les algorithmes intelligents pour offrir une expérience clé en main pour les cas d'utilisation suivants :
  - la visibilité omniprésente en temps réel sur l'ensemble de votre infrastructure de centre de données,
  - l'aperçu précis des communications entre les composants des applications selon leur comportement,
  - le regroupement automatique des points d'extrémité similaires (exemple : grappes de serveurs Web, grappes de bases de données, etc.),
  - les recommandations en matière de politique de liste blanche au niveau des applications pour surveiller les écarts de conformité en quelques minutes,
  - l'analyse des incidences de la politique pour la tester avant son application dans le réseau,
  - la conservation des données à long terme pour permettre une analyse historique sans perte de granularité,
  - l'investigation détaillée grâce à la fonction de demandes de recherche visuelle et en langage naturel.
- **Couche de visualisation :** la plateforme Cisco Tetration Analytics permet la consommation de ces données grâce à une interface graphique utilisateur Web facilement navigable et grâce aux API de transfert d'état représentationnel (REST). En outre, elle fournit une interface de notification à laquelle les systèmes d'interfaces des couches supérieures peuvent se connecter pour recevoir les notifications concernant les flux de trafic, la conformité aux politiques, etc.

Déploiement et gestion des détecteurs

La plateforme Cisco Tetration Analytics est conçue pour fonctionner uniquement avec les détecteurs de logiciels ou avec les détecteurs de matériel. Il est préférable d'activer les deux types de détecteurs (matériel et logiciels), si possible, pour les raisons suivantes :

- Les détecteurs de logiciel fournissent les détails contextuels relatifs au processus.
- Les détecteurs de matériel fournissent les renseignements concernant la mémoire tampon, les mises en correspondance des points d'extrémité de tunnel et la capacité de détecter des rafales du trafic.
- Les mesures précises de la latence du réseau et de l'application.
- L'identification des pertes de paquets au sein d'un flux et de leurs causes.

Figure 2. Télémétrie de Cisco Tetration : détecteurs de matériel contre détecteurs de logiciel



Le déploiement initial des détecteurs s'effectue par une méthode d'automatisation existante que vous possédez (Ansible, Puppet, Chef, etc.). Une fois que le détecteur est installé et se connecte à la plateforme Cisco Tetration Analytics, toute gestion ultérieure, comme les mises à niveau, peut être effectuée grâce à l'interface graphique utilisateur de Cisco Tetration Analytics.

Fonctionnalités et avantages

Le tableau 1 répertorie les fonctionnalités et avantages principaux de la plateforme Cisco Tetration Analytics.

Tableau 1. Fonctionnalités et avantages principaux

Fonctionnalités	Avantages
Détecteurs légers	• La combinaison des détecteurs de matériel et de logiciels détecte tout le trafic transversal et élimine les angles morts. • Les détecteurs de logiciels et de matériel se trouvent à l'extérieur du chemin des données et n'ont pas d'incidence sur les performances applicatives. • Le trafic des détecteurs ajoute moins de 1 % de surcharge sur la bande passante.
Renseignements télémétriques complets	• La télémétrie détaillée permet des analyses comportementales des applications et de leurs écarts de comportement. • Sans aucune charge chiffrée ou non chiffrée. • Les renseignements contextuels de flux avec les données d'en-tête de paquet permettent une meilleure analyse.
Visibilité en temps réel sur le flux	• Recherche de dizaines de milliards de flux et obtention d'une analyse pratique en moins d'une seconde. • Dépannage et détection des anomalies plus rapides pour des opérations en centre de données plus efficaces. • Identification efficace des écarts de comportement des applications et meilleure gestion de la conformité à la politique de réseau.
Prise en charge de l'évolutivité du centre de données	• Collecte de la télémétrie dans chaque paquet du centre de données sans aucun échantillonnage. • La plateforme peut gérer des millions d'unités de flux par seconde. • La conservation des données à long terme facilite les opérations d'investigation et d'analyse.
Facilité de déploiement et d'utilisation	• Fonctionne en tant que dispositif de soutien clé en main pour les cas d'utilisation opérationnelle essentiels. • L'apprentissage automatique sans supervision réduit la nécessité d'une interaction humaine.
Sécurité de la plateforme	• L'accès utilisateur est régi par le contrôle d'accès par rôles (RBAC) pour l'interface graphique utilisateur et pour l'API REST. • La communication entre les différents composants de la plateforme est totalement sécurisée grâce à un pare-feu intégré.

Auto-surveillance de la plateforme	• L'autosurveillance élimine la nécessité d'une grande expertise interne en données volumineuses pour la mise en œuvre de cette plateforme. • La portée de la surveillance s'étend jusqu'aux détecteurs pour faciliter les opérations. • Une option supplémentaire permet d'activer la fonction d'assistance Cisco[MD] Call Home pour signaler les états d'erreur connus.
Interface ouverte	• L'API REST ouverte permet l'intégration des systèmes d'interfaces de couches supérieures. • Le mécanisme de notification permet de surveiller plus facilement les événements selon leur conformité et de détecter les anomalies.

Cas d'utilisation pour centre de données

Les caractéristiques et fonctionnalités de Cisco Tetration Analytics prennent en charge les cas d'utilisation essentiels suivants pour les opérations de centres de données et pour la sécurité de ces derniers :

- visibilité des applications et aperçu de la communication des composants des applications,
- recommandations automatiques en matière de politique de liste blanche et analyse des incidences,
- conformité à la politique et vérifiabilité,
- visualisation du flux, investigation et analyses complètes.

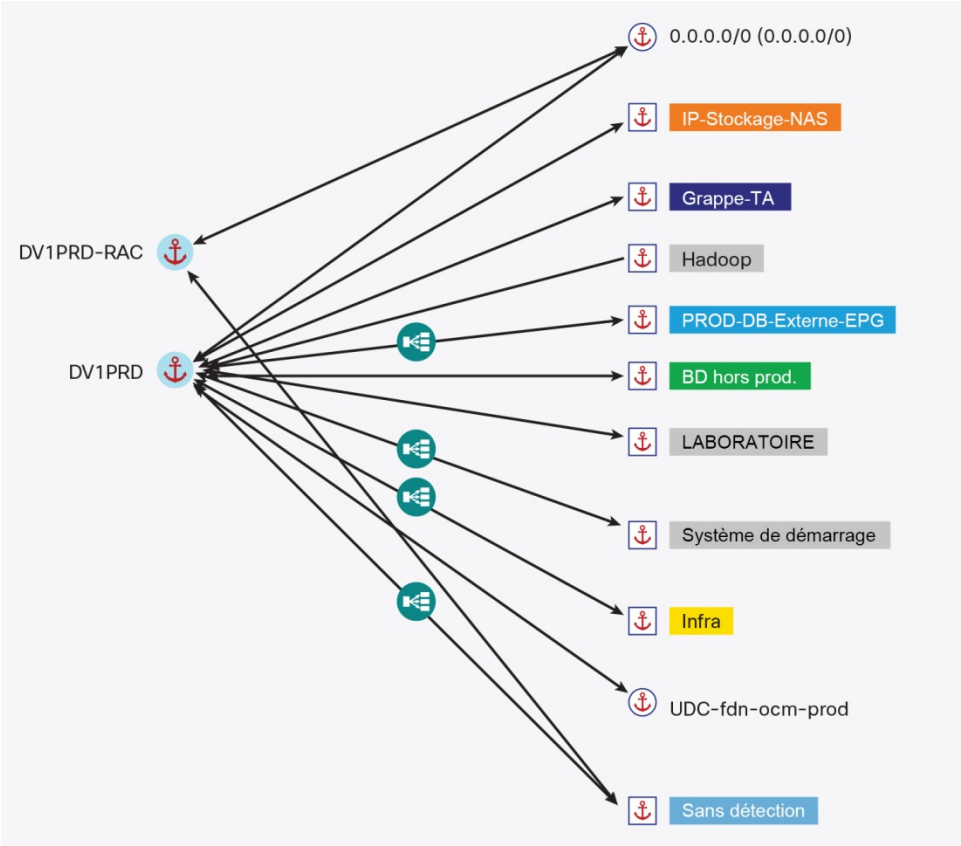
Cisco Tetration AppInsight

Vous devez comprendre les composants des applications et leurs dépendances au sein du centre de données pour pouvoir efficacement exploiter et faire migrer les applications, pour exécuter la planification des reprises après sinistre et pour appliquer la politique de centre de données. La fonctionnalité Cisco Tetration AppInsight traite en temps réel les données sur la communication entre les composants des applications et les algorithmes d'analyses comportementales pour identifier les groupes d'applications et leurs modèles de communication et les dépendances de service (Figure 2). Cette fonction d'analyse des applications permet aux utilisateurs et aux administrateurs de :

- regrouper les hôtes des points d'extrémité et les grappes d'application pour créer des vues d'applications,
- comprendre avec précision les relations entre consommateurs et fournisseurs en fonction des modèles de communication,
- comprendre les dépendances de service pour chaque composant,
- associer les étiquettes et les balises aux points d'extrémité pour faciliter la compréhension.

Les entreprises peuvent également intégrer des renseignements d'appareils tiers de manière intelligente, comme les équilibreurs de charge, pour conserver une vue de bout en bout des communications entre applications.

Figure 3. Carte de Cisco Tetration AppInsight dans l'interface graphique utilisateur Web

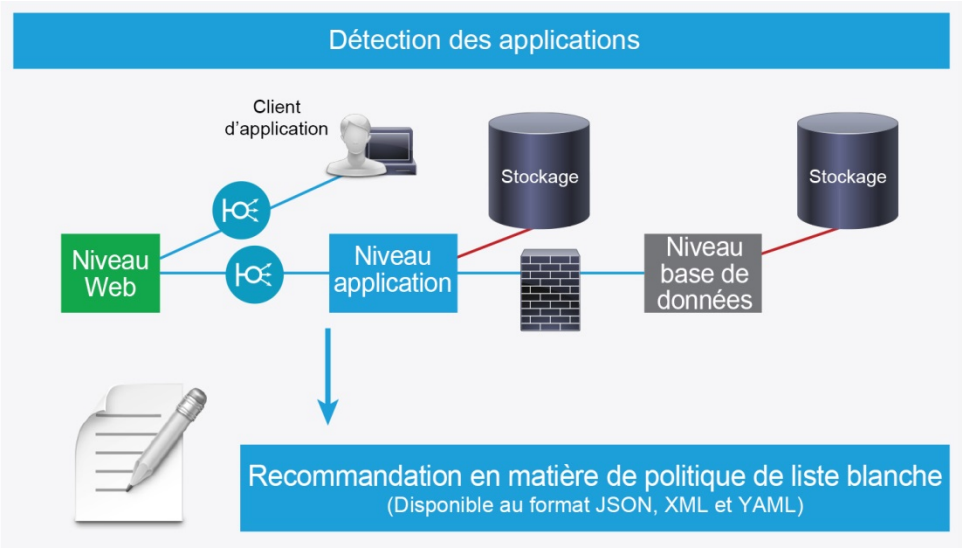


Génération automatisée de politique de liste blanche et conformité

Les entreprises doivent pouvoir générer automatiquement un modèle fiable de politique de liste blanche et mettre ce dernier à jour presque en temps réel à mesure que les applications évoluent. Cette capacité renforce la sécurité et permet d'appliquer une politique cohérente sur différents environnements, y compris dans les charges de travail exécutées dans le nuage. Elle facilite également l'identification des anomalies.

Grâce à la plateforme Cisco Tetration Analytics, vous pouvez générer automatiquement des recommandations en matière de politique de liste blanche en fonction de la communication réelle entre les points d'extrémité. Les recommandations en matière de politique peuvent être exportées dans trois formats de programmation : JSON, XML et YAML. La politique peut être importée dans un contrôleur basé sur la politique, comme le contrôleur APIC (Cisco Application Policy Infrastructure Controller), pour la mise en application et la conformité (figure 3).

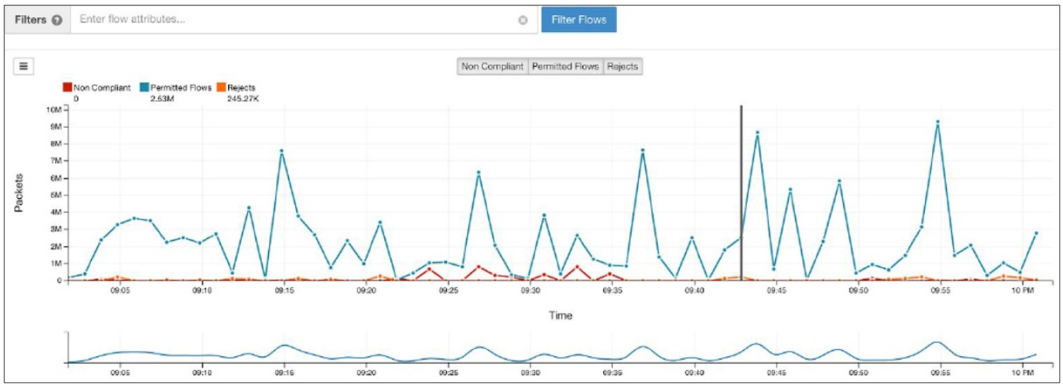
Figure 4. Exportation automatisée de politique de liste blanche



Simulation de politique et analyse des incidences

Grâce à une plateforme Cisco Tetration Analytics, un administrateur peut simuler la politique de liste blanche et en évaluer l'incidence avant de l'appliquer dans le réseau de production. Cette analyse des incidences peut être effectuée en utilisant les données historiques ou les données en temps réel sans conséquences sur le trafic de production. Cette fonctionnalité permet à l'administrateur de voir quelle incidence aurait cette politique de liste blanche sur le trafic réel passant dans le réseau. En outre, l'administrateur peut immédiatement visualiser les flux qui seront considérés comme conformes ou non conformes ou annulés (figure 4). L'administrateur peut utiliser cette simulation et ces analyses pour régler la mise en correspondance des applications et pour actualiser la politique de liste blanche pour qu'elle corresponde avec précision au comportement des applications.

Figure 5. Aperçu de la conformité aux politiques dans la plateforme Cisco Tetration Analytics

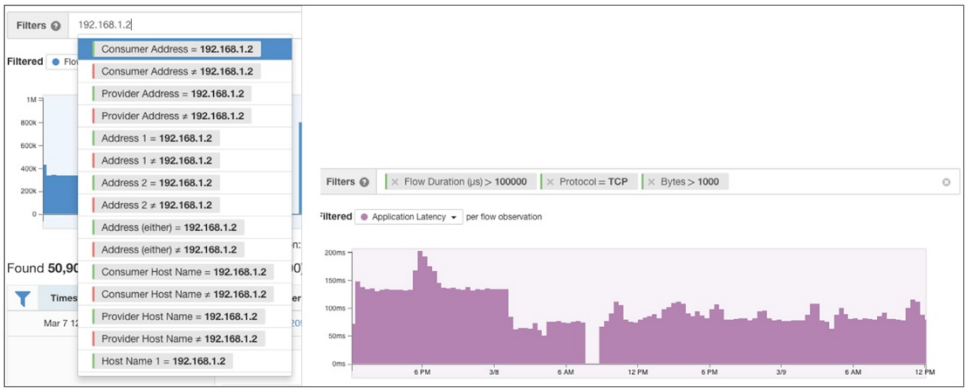


Visualisation et exploration des flux

La plateforme Cisco Tetration Analytics remplace un moteur de recherche pour tous les flux dans votre centre de données. La fonction de recherche fournie par la plateforme est d'une puissance inégalée et permet à l'utilisateur de rechercher des dizaines de milliards d'enregistrements de flux en moins d'une seconde. Elle permet également d'effectuer des demandes de recherche détaillée, visuelle et en langage naturel,

pour trouver les détails qui sont essentiels aux opérations de centre de données. Cette fonction de recherche vous permet de trouver non seulement tous les problèmes connus, mais également des comportements anormaux qui autrement peuvent passer inaperçus (figure 5).

Figure 6. Investigation et recherche de flux de l'interface graphique utilisateur Web de Cisco Tetration Analytics



Autosurveillance de la plateforme

Les capacités d'autosurveillance de Cisco Tetration Analytics vous permettent de facilement gérer et exploiter cette plateforme sans aucune expertise en données volumineuses. La portée de cette capacité s'étend jusqu'aux détecteurs pour faciliter l'application du SLA. Les capacités d'autosurveillance de la plateforme comprennent :

- la surveillance des flux de pipeline de la plateforme et des retards,
- la surveillance du statut et de l'état de chaque composant de la plateforme,
- la surveillance de l'état du détecteur, de l'UCT et de la bande passante,
- la fonctionnalité d'assistance facultative Call Home pour les erreurs connues.

Prise en charge et compatibilité de la plateforme

Les tableaux 2 et 3 présentent la prise en charge et les renseignements sur la compatibilité des logiciels et matériels pour la plateforme Cisco Tetration Analytics.

Tableau 2. Détecteurs de logiciels et systèmes d'exploitation pris en charge

Mode serveur	Système d'exploitation	Fournisseur et version
Machines virtuelles et serveurs sans système d'exploitation	Linux	• Serveur Red Hat Enterprise version 5.3 et ultérieure • Serveur Red Hat Enterprise version 6.0 • CentOS version 5.11 et ultérieure • CentOS version 6.0 • Ubuntu version 12.04, 14.04 et 14.10
	Microsoft Windows Server	• Microsoft Windows Server 2008, Édition Standard, Enterprise, Essentials et pour centre de données • Microsoft Windows Server 2008 R2, Édition Standard, Enterprise, Essentials et pour centre de données • Microsoft Windows Server 2012, Édition Standard, Enterprise, Essentials et pour centre de données • Microsoft Windows Server 2012 R2, Édition Standard, Enterprise, Essentials et pour centre de données

Tableau 3. Détecteurs de matériel pris en charge

Gamme de produits	Plateforme	Version logicielle Cisco NX-OS
Commutateurs Cisco Nexus, série 9000	Cisco Nexus 92160YC-X	NX-OS version 7.0(3)I3(1) et ultérieure
	Cisco Nexus 93180YC-EX et Cisco Nexus 93108TC-EX	NX-OS version 7.0(3)I4(2) et ultérieure

Caractéristiques techniques du produit

Le tableau 4 présente les caractéristiques des composants de la plateforme Cisco Tetration Analytics standard. Le tableau 6 présente les caractéristiques d'alimentation.

Tableau 4. Plateforme Cisco Tetration Analytics

La plateforme Cisco Tetration Analytics standard comprend 36 serveurs et 3 commutateurs. Ces trois commutateurs permettent aux serveurs d'accéder à l'ensemble du réseau CLOS.

Matériel de la plateforme	Quantité
Nœuds de traitement (serveurs) de Cisco Tetration Analytics	16
Nœuds de base (serveurs) de Cisco Tetration Analytics	12
Nœuds de service (serveurs) de Cisco Tetration Analytics	8
Commutateurs Cisco Nexus 9372PX	3

Tableau 5. Caractéristiques d'alimentation

Propriété	Plateforme Cisco Tetration Analytics
Puissance de crête pour la plateforme Cisco Tetration Analytics (option de bâti unique à 39 RU)	22,5 kW
Puissance de crête pour la plateforme Cisco Tetration Analytics (option à double bâti à 39 RU)	11,25 kW par bâti (total de 22,5 kW)

Renseignements relatifs à la commande

Le tableau 6 fournit les UGS d'offres groupées de matériel et de logiciel pour une grande plateforme de démarrage Cisco Tetration Analytics

Tableau 6. Renseignements relatifs à la commande : offres groupées de matériel

Référence	Description
TA-CL-G1-39-K9	Plateforme Cisco Tetration Analytics standard avec 36 serveurs et 3 commutateurs prenant en charge le traitement de la collecte de la télémétrie de Tetration comptant jusqu'à 5 000 points d'extrémité uniques (machines virtuelles ou serveur sans système d'exploitation) ou jusqu'à 1 million d'unités d'événements de flux par seconde, selon la plus faible de ces valeurs.

Le tableau 7 fournit les UGS de licence d'utilisation de logiciel pour chaque point d'extrémité.

Tableau 7. Renseignements relatifs à la commande : licence d'utilisation de logiciel pour les points d'extrémité uniques

Référence	Description
TA-BASE-5K-K9=	PID de la licence d'utilisation de logiciel de Tetration Analytics pour la collecte de la télémétrie de Tetration comptant jusqu'à 5000 points d'extrémité uniques (machines virtuelles ou serveur sans système d'exploitation) ou jusqu'à 1 million d'unités d'événements de flux par seconde, selon la plus faible de ces valeurs.

Profitez de l’expertise de Cisco pour accélérer votre réussite

Cisco offre des services professionnels et des services d’assistance afin de permettre aux entreprises de tirer pleinement parti de la plateforme Cisco Tetration Analytics. Les experts des services Cisco vous aident à intégrer la plateforme dans votre environnement de production du centre de données, à définir les cas d’utilisation adaptés à vos objectifs commerciaux, à configurer l’apprentissage automatique et à valider les politiques et la conformité pour améliorer les performances applicatives et les performances de fonctionnement. Le service d’assistance pour la solution Cisco Tetration Analytics offre une assistance matérielle et logicielle, ainsi qu’une assistance au niveau de la solution. Un contrat annuel couvre tous les besoins d’assistance. L’expertise dans les services Cisco Tetration Analytics vous permet de profiter des avantages suivants : accélération de la rentabilisation des investissements, adoption exhaustive dans votre environnement, politiques et performances applicatives optimisées et assistance pour l’ensemble de la solution.

Le financement Cisco Capital pour vous aider à atteindre vos objectifs

Le financement de Cisco Capital[MD] peut vous aider à acheter la technologie dont vous avez besoin pour atteindre vos objectifs et demeurer concurrentiel. Nous pouvons vous aider à réduire vos dépenses d’investissement (CapEx), à accélérer votre croissance et à optimiser les dollars investis et le rendement du capital investi. Le financement de Cisco Capital vous donne la flexibilité d’acquérir le matériel, les logiciels, les services et les équipements complémentaires de tiers indépendants. Et vous n’aurez qu’un seul paiement prévisible à faire. Le financement Cisco Capital est offert dans plus de 100 pays. Pour en savoir davantage.

Pour obtenir de plus amples renseignements

Pour de plus amples renseignements sur la plateforme Cisco Tetration Analytics, rendez-vous à la page http://www.cisco.com/go/tetration ou communiquez avec votre représentant Cisco local.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (USA) Pad Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l’adresse www.cisco.com/go/offices.

Imprimé aux États-Unis C78-737256-00 06/16