NetCrunch - Concepts clés

NetCrunch est conçu pour gérer des milliers de composants. Il vous permet les gérer avec des règles et non pas individuellement. NetCrunch effectue beaucoup de tâches automatiquement, ce qui vous permet de configurer plusieurs centaines de nœuds en quelques minutes. Cela peut être un choc si vous êtes habitué à travailler avec des outils nécessitant une configuration individuelle.

Haute performance

NetCrunch combine les technologies les plus avancées pour le meilleur résultat: une base de données NoSQL exclusive pour les valeurs de performance du réseau, une base de données en mémoire pour le statut des systèmes en temps réel et une base de données SQL embarquée pour stocker les alertes. L'évolutivité sur une machine unique, possédant plusieurs processeurs et plusieurs gigaoctets de RAM, est impressionnante. Il peut surveiller plus de 600.000 paramètres de performance sur un seul serveur.

- Plus de 600.000 sondes par serveur
- Pas de limite sur les données stockées
- Les données de performances brutes sont stockées
- Fonctionne en environnement virtuel
- Fonctionne dans un cluster Fault Tolerance vSphere

Gestion automatique par règles

NetCrunch vous permet de détecter automatiquement les nœuds à intervalles réguliers. Une fois un système découvert, NetCrunch scanne ses services réseau, détermine sa nature et si il prend en charge le SNMP. Les réglages de surveillance peuvent être gérés à l'aide de *packs de monitoring* qui définissent des éléments à superviser et déclenchent des alertes quand certaines conditions sont réunies. Les packs de monitoring peuvent être affectés aux équipements manuellement ou automatiquement selon des règles (basées sur le type d'appareil ou autres critères). Le programme gère également de nombreuses cartes et tableaux de bord, et crée automatiquement: cartes, cartes de routage du réseau logique et cartes de segment physique (couche 2)

- Découverte automatique des plages IP
- Découverte automatique des services réseau
- Découverte du type de périphérique

Construit pour la cohérence

NetCrunch a été créé pour un traitement et une visualisation uniforme des données. Dans un outil basé sur capteurs ou scriptes, la logique de surveillance se trouve au niveau des capteurs ce qui rend difficile leur gestion et leur mise à jour. NetCrunch centralise la logique de surveillance. Les moteurs de supervisions fournissent des données et des événements et tout leur s'effectue par le serveur. Cela signifie que les fonctionnalités comme les alertes conditionnelles ou les différents types de déclencheur sont disponibles pour tous les événements et les données de performance. NetCrunch permet à la fois la création et l'utilisation de scriptes simples et de logiques plus complexes s'appuyant sur l'état des objets.

- Traitement uniforme pour toutes les sources de données
- Visualisation homogène
- Courbe d'apprentissage rapide

Flexibilité et personnalisation

Il est impossible d'énumérer tous les aspects pouvant être personnalisés dans NetCrunch! Par exemple, la console prend en charge plusieurs moniteurs, permet l'amarrage de fenêtres et peut passer automatiquement en plein écran. Vous pouvez créer des cartes avec des widgets montrant les données ou l'état en temps réel et vous pouvez gérer les notifications par le biais des groupes et des profils utilisateurs (avec intégration AD). Vous pouvez également exporter les données de NetCrunch, construire des scriptes personnalisés ou obtenir des données à partir d'une page Web.

- Compteurs de performance calculés
- 8 types de déclencheurs de performance
- Alertes conditionnelles
- Affichages personnalisés
- Support pour scriptes et API
- Escalade pour alerte
- Compilateur de MIB
- Support multi écran et amarrage de fenêtre
- Mode plein écran automatique

Supervision

La surveillance du réseau NetCrunch est construite sur deux blocs de base: indicateurs de performance et événements. Puisque chaque moteur de supervision ne délivre que des événements et des métriques, vous pouvez appliquer les mêmes conditions et les mêmes types déclencheur à chacun d'eux. NetCrunch ne nécessite pas d'agent à installer. NetCrunch est également extensible à l'aide de scriptes et des données externes peuvent être intégrées dans NetCrunch via HTTP.

SNMP

NetCrunch utilise SNMP pour la gestion des périphériques réseau (commutateurs, imprimantes, etc.). Le programme supporte les traps SNMPv3, traps infos paquets et peut les transférer. Il comprend également un compilateur MIB et plus de 3500 MIB pré-compilés.

- SNMP v1, v2c, v3
- SNMP v3 notifications et info
- Compilateur de MIN SNMP
- 3500+ MIBs pré-compilés

Supervision commutateurs et routeurs

NetCrunch supporte différents aspects de la surveillance des commutateurs et des routeurs, y compris l'état des interfaces et la bande passante. Le programme identifie automatiquement les connexions de la couche physique et permet le mappage des ports. Notre sonde Cisco IP SLA permet de surveiller l'état des opérations IP SLA et des compteurs de performance associés. NetCrunch supporte également le contrôle et l'analyse du trafic et la technologie Cisco NBAR.

- Surveillance de la bande passante
- Suivi de l'interface
- Cartes de routage
- Mappage de ports avec VLAN
- Cartes couche physique
- Surveillance du trafic
- Sonde IP SLA
- Surveillance VOIP

Supervision serveur et système d'exploitation

NetCrunch supporte la supervision sans agent de systèmes type Unix (Linux, Solaris, BSD et Mac OS X) en utilisant le protocole SSH. Le programme inclus des packs de supervision prédéfinis pour chaque OS. La supervision Windows est intégrée avec l'Active Directory et ne nécessite aucun agent SNMP à installer sur le serveur. Il permet la supervision sous Windows des performances, des services et du journal d'événements. Vous pouvez également surveiller les fichiers et dossiers sous Windows (natif) et d'autres systèmes (via FTP/S ou HTTP/S). Tous les moteurs de supervision prennent en charge les mesures de performance, les processus et la supervision des connexions réseau.

- Supervision des serveurs Windows
- Supervision des serveurs Linux
- Supervision des serveurs Mac OS X
- Supervision des serveurs BSD, FreeBSD et OpenBSD
- Supervision des services réseau, des processus, des événements et des mesures de performance

Supervision des services réseau et applications

NetCrunch supervise plus de 65 services TCP/UDP prédéfinis tel que DNS, FTP, HTTP, POP3, SMTP, etc. Pour chaque service, NetCrunch peut vérifier la connectivité ou les schémas de réponse afin de valider leur bon fonctionnement. NetCrunch peut surveiller une boîte courriel ou envoyer un courriel de test afin de vérifier les fonctionnalités des serveurs de messagerie. Toutes les sondes prennent en charge les connexions sécurisées. Les sondes fichiers et dossiers utilisent pour accéder aux fichiers distants SMB(Windows), FTP(/S) et HTTP(/S).

- Plus de 65 modèles de services réseau
- Création de contrôle de services réseau personnalisés
- Sonde Apache
- Sonde de fichiers de protocole
- Sonde dossier
- Sonde page Web
- Sonde requête HTTP
- Sonde courriel
- Sonde requêtes DNS

Supervision NetFlow

NetCrunch comprend un serveur de flux qui vous permet de collecter et de surveiller les informations sur le trafic réseau à partir de diverses sources de flux en utilisant: IPFix, NetFlow (v5 et v9), JFlow, sFlow, Netstream, cflow, AppFlow et les protocoles de rFlow. Le programme analyse le trafic avec diverses catégories, y compris les applications, les protocoles et les catégories de domaine. NetCrunch supporte Cisco NBAR et vous permet de créer des définitions des catégories d'applications personnalisées.

- Supervision NetFlow v5, v9
- Supervision IPFix
- Supervision JFlow, sFlow, netStream, AppFlow et rFlow
- Supporte Cisco NBAR v2
- Regroupement des applications personnalisé

Supervision des journaux des événements

NetCrunch vous permet de collecter et de réagir à des événements provenant de sources diverses. Il peut recevoir différents traps SNMP (y compris les notifications en version 3) et peut agir comme un serveur syslog. En outre, NetCrunch peut collecter des données à partir du journal des événements Windows via WMI ou de journaux de texte utilisant notre sonde de fichiers texte.

- Serveur Syslog
- Réception de trap SNMP
- Journal des événements Windows
- Sonde pour fichiers texte

Inventaire matériel et logiciel

NetCrunch peut collecter des informations d'inventaire à partir des nœuds Windows à l'aide de WMI. L'inventaire recueille des données détaillées sur le matériel, le système d'exploitation et les logiciels installés. Le programme affiche également des informations sur tous les patchs installés.

- Détails Hardware & OS
- Logiciels installés
- Correctifs installés
- Journal des modifications
- Comparaison dans le temps ou entre des nœuds

Supervision personnalisée

Dans NetCrunch vous pouvez planifier l'obtention de données à partir du serveur, d'un serveur Web ou une application supportant les requêtes HTTP GET. En guise de réponse, NetCrunch attend des données JSON ou XML au format Open Monitor. Vous pouvez également envoyer des données à l'aide de l'interface REST, simple à mettre en oeuvre avec curl ou tout autre langage de programmation, y compris les langues populaires comme Java, C #, Javascript ou Python. Voir des exemples sur Github

- Exécution planifiée sur le serveur NetCrunch Exe, JScript ou VBScript
- Envoi de données à l'aide d'une interface programmatique NetCrunch
- Exemples sur GitHub

Support multi-vendeur

NetCrunch inclut le support pour les technologies Cisco, VMware et Microsoft car ils sont nos partenaires technologiques.

Le programme prend en charge différentes technologies Cisco, y compris la surveillance VOIP utilisant les opérations IP SLA définies sur les périphériques Cisco. Le serveur NetCrunch Flow supporte la technologie NetFlow et Cisco NBAR.

NetCrunch supervise VMware ESXi 5.5/6 y compris la surveillance de l'état du matériel et des machines virtuelles. Pour les applications les plus populaires comme MS SQL et Exchange, NetCrunch offre plus de 100 packs de monitoring, ensembles de règles de supervision prédéfinies.

- Supervision Cisco
- Supervision Microsoft
- Supervision VMWare
- Supervision NetApp
- Supervision HP
- Supervision IBM
- Supervision Oracle
- APC, Avaya, Juniper et plus encore...

Supervision avancée

NetCrunch utilise des techniques avancées afin de minimiser les fausses alertes, en particulier lors de la surveillance des périphériques distants et des connexions intermédiaires. La définition des dépendances permet de surveiller les connexions et de supprimer toutes les fausses alertes. Le programme privilégie également la supervision de l'infrastructure réseau par rapport aux points de terminaison distants. Les packs de monitoring simplifient la gestion des paramètres de surveillance et permet d'établir des règles pour surveiller des groupes d'équipement au lieu d'être obligé de configurer chaque nœud un par un.

Alarme

Différentes source d'événements

NetCrunch est la première source qui génère diverses événements représentant un changement d'état (up/down), un déclencheur activé sur une métrique de performance, l'état d'une sonde ou d'un moteur de supervision. Le programme est également capable de recevoir des événements externes en appliquant des règles et des filtres. Ainsi vous pouvez créer des alertes sur les traps SNMP reçus, les messages Syslog ou les événement provenant du journal des événements Windows. NetCrunch garde toutes ces alertes dans une base de données intégrée SQL.

- NetCrunch événement d'état
- NetCrunch Sonde
- Déclencheur d'alerte pour performance
- Journal d'événements Windows
- Messages Syslog
- Traps SNMP & Notifications

Déclencheurs pour métriques de performance

L'un des éléments de base de la surveillance du réseau est le suivi de diverses mesures de performance. Indépendamment de l'origine de la métrique, les utilisateurs peuvent toujours utiliser le même ensemble de conditions pour déclencher des alertes sur les valeurs réelles ou leur moyenne. La moyenne peut être calculée à partir d'un nombre de valeurs ou dans un laps de temps défini.

- Seuil de déviation
- Seuil de référence
- État
- Constance
- Valeur existante ou manquante
- Delta
- Fourchette

Corrélation des alertes

NetCrunch supporte différents types de corrélations pour les alertes. Chaque événement généré par NetCrunch a un début et une fin, de sorte que vous pouvez facilement attribuer une action à l'ouverture et à la fermeture de l'alerte. Ceci permet de se concentrer principalement sur les problèmes non résolus. Les autres événements reçus peuvent être corrélés manuellement en ajoutant des conditions liées à la fermeture des alertes. La corrélation avancée vous permet également de déclencher des alertes uniquement si plusieurs événements se produisent dans un

intervalle de temps donné, ou quand ils sont en attente simultanément. Par exemple, cela vous permet de définir une alerte uniquement si deux interfaces redondantes sont hors-service.

- Corrélation automatique des alertes en attente
- Corrélation manuelle des événements externes
- Corrélation avancée

Alertes conditionnelles

La condition la plus simple est de déclencher une alerte quand sa condition est réunie. Mais qu'en est-il lorsque un événement ne se produit pas? Comme une sauvegarde planifiée? Parmi les possibilités d'alerte de NetCrunch, vous pouvez définir des alertes pour des événements ne survenant pas dans un laps de temps défini ou après un temps d'attente pour remarquer quand une pulsation régulière s'arrête. D'autre condition permettent de stopper le déclenchement d'action pour un temps défini. Par exemple, la perte de courant ne devrait créer une alerte qu'après plusieurs minutes pour éviter d'alerter inutilement si le courant est rétabli rapidement.

- Lors de l'événement
- Si l'événement se produise après un temps x
- Si l'événement se produise plus x fois
- Dans un intervalle de temps
- En dehors d'un intervalle de temps
- Si l'événement ne survient pas pendant un temps donné
- Si l'événement n'est pas arrivé après un temps x
- Si l'événement est en attente plus de x

Actions d'alertes

NetCrunch supporte diverses actions, notamment: notifications, audit, actions de contrôle et scripts distants. Les notifications sont très flexibles et sont contrôlées par les profils utilisateurs. En outre, elles peuvent être combinées avec les cartes de l'atlas de telle sorte qu'il est possible d'envoyer des notifications différentes groupes en fonction des attributs du système responsable de l'alerte. Les actions d'audit permettent d'écrire les événements dans un fichier, dans le journal des événements Windows, d'envoyer des traps SNMP, des messages Syslog ou de déclencher des webhooks. Enfin, les actions a distance peuvent être exécutées sur Windows, Linux, Mac OS X et BSD y-compris le redémarrage et l'arrêt de services ou du système.

- Notifications par courriel ou SMS
- Actions de contrôle (Redémarrage et, exécution, arrêt, etc)
- Audit (Syslog, traps SNMP, journam d'événements Windows, fichier)
- Exécution de scriptes et programmes à distance
- 35 actions d'alertes prédéfinies disponibles

Escalade & Exécution conditionnelle

Les actions peuvent être exécutées immédiatement ou, tant que l'alerte n'a pas été fermée, avec un délai. Cela permet de planifier un processus d'escalade dans le temps. La dernière action peut être répétée afin de rappeler tant que nécessaire que le problème demeure. En outre, vous pouvez spécifier des actions à exécuter automatiquement lors de la fermeture de l'alerte. Chaque action peut être limitée, de manière automatique ou manuelle, par les attributs du système l'ayant déclenchée, par exemple son appartenance à certaines vus de l'atlas mais aussi en fonction du temps. Cela vous permet de créer des scriptes d'alerte flexibles, par exemple l'envoi de notifications différentes en fonction de l'emplacement du nœud. Les scriptes d'alerte définis peuvent être utilisés pour plusieurs alertes et intègre la criticité du système pour éventuellement restreindre leur exécution.

- Exécution à l'ouverture de l'alerte ou après un temps donné
- Exécution à la fermeture
- Exécution en fonction de la criticité
- Exécution en fonction du temps
- Exécution en fonction des attributs du système

Traitement avancé des alertes

NetCrunch utilise diverses technologies pour éviter les fausses alertes ou protéger contre les surcharges pouvant être causées par un dysfonctionnement d'un appareil défectueux. Quand un système envoie des messages Syslog ou traps SNMP, NetCrunch attend quelques secondes pour ne déclencher qu'une seule alerte quand le même message apparaît plusieurs fois. Une autre technique (*suppression d'événements*) est utilisée pour détecter les fausses alertes dont la cause est la défaillance de systèmes intermédiaires.

Visualisation

L'atlas réseau

L'atlas réseau dans NetCrunch est un référentiel central de toutes les cartes afin de regrouper les nœuds en différentes catégories comme: nœuds d'une plage IP, nœuds d'un seul segment de la couche 2, ou nœuds situés dans une zone identique. Il vous permet de créer manuellement et automatiquement de nombreuses vues personnalisées.

- Vues dynamiques
- Dossiers de vues dynamiques
- Vues personnalisées
- Cartes, top charts et vues de performance

Dashboards

Chaque vue de l'atlas réseau possède son tableau de bord personnalisable. La vue Top Charts regroupe les informations de tous les nœuds surveillés, tandis que le tableau de bord d'une carte affiche des informations filtrées par groupes de nœuds (comme type de système ou emplacement).

- Synthèse d'état
- Top Charts

Vues temps réel

La plupart des vues NetCrunch sont en temps réel et mises à jour automatiquement. Elles peuvent également être organisées automatiquement. Les cartes de couche 2 indiquent l'état des ports et peuvent aussi montrer le trafic actuel et le volume agrégé pour chaque ports. Les dépendances de surveillance sont représentées à l'aide d'un schéma pouvant être établi automatiquement à partir des informations collectées sur les routeurs et commutateurs. Des cartes personnalisées avec des widgets peuvent indiquer l'état des objets du réseau (nœuds, interfaces, services, alertes, etc.) et des mesures de performance actuelles.

- Cartes couche 2
- Carte du routing
- Dépendances de surveillance
- Cartes personnalisées
- Carte de performance

Widget carte graphique

Les cartes graphiques sont des éléments essentiels de la visualisation du réseau. Contrairement à un tableau de bord composé de carreaux, ces éléments graphiques montrent les relations entre les éléments et leur emplacement. Les cartes dans NetCrunch peuvent contenir des éléments pour visualiser l'état d'un objet ou présenter des données de performance.

- État de nœud
- État de service
- État d'interface
- État pack de monitoring
- État de sonde
- État d'alerte
- 5 widgets de données de performance

Vues alertes & événements

Dans NetCrunch, la fenêtre la plus importante est celle qui présente les alertes actuelles. Elle vous aide à ne se concentrer que sur les problèmes encore en cours au lieu de présenter toutes les alertes. La fenêtre présentant l'historique contient toutes les alertes traitées par NetCrunch et stocke également des données de performance récoltées au moment de l'alerte. NetCrunch offre dans l'historique de nombreuses vues prédéfinies et vous permet de définir vos propres vues à l'aide d'un outil de création de filtres intuitif. La fenêtre de synthèse donne un bref aperçu du nombre d'alertes par catégorie dans un intervalle de temps donné.

- Alertes en cours
- Résumé des alertes par catégorie
- Historique des événement avec vues personnalisées
- Aperçu des performances

État du nœud & Détails

La fenêtre d'état du nœud résume rapidement toutes les informations concernant un système. Cette synthèse présente les éléments surveillés et leur état, ainsi que des informations sur le système comme son type ses paramètres de base (par exemple la mémoire, le disque et l'utilisation du réseau pour un serveur). Sous l'onglet performance, vous pouvez voir les valeurs actuelles, la dernière heure et les 24 dernières heures. La fenêtre affiche différents onglets en fonction du type de nœud.

- Résumé de l'état
- Graphes de performance
- Services réseau
- Interfaces
- Mappage de ports sur ses commutateurs

- Etat du matériel pour l'ESX
- Opérations IP SLA
- Dépendances
- Alertes en attentes et historique des événements

Outils supplémentaires

NetCrunch offre des outils supplémentaires pour l'exploration des données. Le navigateur SNMP vous permet de parcourir les données SNMP simplement avec des vues spécifiques pour chaque dispositif. Cet outil vous permet également de définir ou modifier des variables SNMP. L'outil WMI vous permet de parcourir à distance les informations WMI. Le navigateur de performance et tendance est accessible pour toutes les données collectées: nœud, tableau de bord et vues de performance. Enfin, vous pouvez personnaliser la liste des outils disponibles dans la console et transmettre des paramètres NetCrunch aux outils externes.

- Navigateur informations SNMP
- Créateur de vues SNMP
- Outil WMI
- Outils IP
- Navigateur de performances et tendances
- Menu d'outils personnalisable

Serveur

Haute performance

NetCrunch serveur fonctionne sur système Serveur Windows x64 (*Windows 2008 R2*, * Windows 2012 R2*). Il est livré avec son serveur Web intégré et une base de données SQL embarqué pour stocker les événements. NetCrunch peut être installé sur une machine virtuelle, à condition de lui attribuer au moins 4 processeurs et 4 Go de RAM. NetCrunch stocke les données dans des bases de données mais traite toutes les données actuelles directement en mémoire ce qui donne des performances supérieures à celles des solutions seulement basées sur SQL.

- Serveur x64 multi threaded avec 4 Go de RAM
- Traitement en mémoire
- Serveur Web (avec support SSL) intégré
- Base de données embarquée
- Fonctionne sur une machine virtuelle
- Supervise plus de 600.000 indicateurs de performance

Zéro administration base de données

NetCrunch est livré avec une base de données SQL intégrée pour stocker les événements générés par NetCrunch ainsi que les événements collectés à partir des traps SNMP, des messages Syslog et journal d'événements Windows (WMI). Pour les données de performance, NetCrunch utilise une base de données exclusive NoSQL, sans limite sur la taille ou la durée de conservation des données. Les données des événements sont accessibles par le pilote ODBC inclus, et les données de performance peut être exportées à l'aide d'un outils spécifique pouvant être planifié pour l'export automatique vers des bases SQL externes.

- Base de données d'événements SQL intégrée
- Base de données de performance NoSQL intégrée
- Aucune limite sur la taille des données de performance

Console

Console d'administration à distance

La console d'administration NetCrunch peut être installée sur un poste de travail Windows à partir de Windows 7 en 32 bit ou 64 bit. Un écran HD large avec support pour des couleurs 32 bit est requis. Profitez de NetCrunch au meilleur de ses capacités avec plusieurs écrans 50 pouces afin de pouvoir présenter plus de détails. Néanmoins, un ordinateur portable moderne avec un écran de 13" pouce et Windows 7 ou 8 vous permettra aussi d'utiliser la console sans souci.
La console présente des informations en temps réel et requiert peu de bande passante car seules les données sont transférées et non pas le flux HTML comme dans beaucoup d'autres solutions. Même avec des latences réseau de plus de 200ms, la console fonctionne correctement. Enfin, vous pouvez configurer le mode diapo en pleine écran pour la visualisation de cartes à intervalle régulier automatique.

- Prise en charge de plusieurs écrans
- Fonctionne sur des liaisons lentes
- Mode plein écran automatique
- Console 32 bits peut être exécutée sur Vista ou version ultérieure
- Prise en charge de l'écran tactile

En déplacement

Vous pouvez surveiller l'état de votre réseau où que vous soyez, en utilisant la console Web NetCrunch via HTTP/S. Elle comprend également un système d'autorisation permettant de limiter les droits et les opérations à des cartes spécifiques. Les comptes utilisateurs de la console Web peuvent utiliser l'Active Directory. Pour une expérience la meilleure avec plusieurs écrans et des données en temps réel, vous pouvez utiliser la console d'administration à distance fonctionnant dans les environnements Windows. NetCrunch dispose également d'un client mobile conçu pour un accès rapide à partir de smartphones et tablettes (iOS, Android, Windows) supportant HTML5.

- Fonctionne avec les navigateurs modernes (IE10 +)
- Client mobile pour iOS, Android, Windows Phone
- Permet le contrôle d'accès et la restriction au niveau des cartes

GrafCrunch

La dernière version de NetCrunch intègre un fork du projet open source *Grafana*. Un des meilleurs projets open source pour la visualisation offrant de nouvelles possibilités pour créer des tableaux de bord de performance en temps réel et permettant la présentation de données provenant de diverses sources. L'installation simplifie l'intégration entre GrafCrunch et NetCrunch en créant automatiquement les données d'identification pour l'accès aux données.

- Fork de Grafana
- Open Source

Licences

Licence basée sur le nombre de nœuds

Le modèle de licence NetCrunch repose uniquement sur le nombre de nœuds surveillés et le nombre de connexions administratives simultanées au serveur. Contrairement à beaucoup de produits, NetCrunch ne limite pas le nombre de paramètres à surveiller (probes).

- Coût réduit
- Simple à gérer
- Pas de limites sur les données
- Pas de limites de détection

Editions

NetCrunch est disponible en deux éditions distinctes: Premium et Premium XE. La différence principale entre ces versions est l'évolutivité. NetCrunch Premium s'adresse au réseau de petite et moyenne taille jusqu'à 300 nœuds. Premium XE comprend en plus: le support pour un nombre de nœuds plus important, un traitement plus intensif (optimisation interne pour exécuter plus de travail), support pour VLAN, alerte conditionnelle, corrélation d'alertes, surveillance IP SLA, suppression d'événements, supervision priorisée et événements externes en cache.

L'édition Corporate permet d'installer un nombre illimité de serveur NetCrunch dans votre entreprise.

- Premium
- Premium XE
- Corporate