

B | DNA



Comprendre l'inventaire

Une approche détaillée de BDNA Discover™

Les DSI qui cherchent à mesurer et à gérer les activités informatiques sont confrontés à un déficit chronique des données dès que l'on parle de technologie. Bien souvent, ils en connaissent peu sur la technologie utilisée, à quels endroits elle se trouve et comment elle est utilisée. Ce livre blanc examine comment la technologie d'inventaire de BDNA permet un recensement rapide, précis et exhaustif des actifs technologiques de l'entreprise.

Vue d'ensemble

L'activité dépend aujourd'hui grandement de la technologie et requiert de la part du service informatique de la transparence et de la responsabilité. Les DSI qui cherchent à mesurer et à gérer les activités informatiques sont confrontés à un déficit chronique de données dès que l'on parle de technologie. On en connaît peu sur le type de technologie déployée, sa localisation et son mode d'utilisation. Des décisions essentielles, voire stratégiques, sont souvent basées sur des informations incomplètes et des hypothèses, et non des mesures et des analyses.

Ce manque de transparence peut avoir une incidence directe sur le succès de l'entreprise. A titre d'exemple, on notera que les coûts d'achats de logiciels d'entreprise pourraient connaître une augmentation, alors que les technologies de virtualisation permettent d'étendre l'utilisation des autres logiciels au-delà de ce qui est prévu dans les licences existantes. On constate souvent dans les entreprises que le choix des produits se fait plus par division & service qu'au niveau de l'entreprise, ce qui empêche de réaliser des économies d'échelle. Et les DSI manquent de visibilité pour planifier les migrations importantes de centres de traitement de données, négocier des accords de sous-traitance ou évaluer les nouvelles technologies de manière significative.

BDNA Discover™ résout ce problème en fournissant au DSI et à la direction de l'information, une vision de la situation telle qu'elle est : la FactBase de BDNA devient un système fiable d'enregistrement de tous les actifs et ressources informatiques. Elle a été créée à partir d'une technologie d'inventaire sans agent, et haut débit.

Inventaire – Description générale

Le concept de BDNA vient de la volonté de fournir de l'aide aux entreprises pour comprendre leur infrastructure technologique afin qu'elles aient l'information nécessaire pour prendre les décisions stratégiques de réduction des coûts informatiques. On est conscient que le DSI a besoin d'un flux d'information instantané et à jour pour la gestion de son activité. Des méthodes manuelles pour recueillir l'information sur les actifs déployés ne sont pas applicables dans l'environnement informatique actuel - le problème est trop large, les actifs trop distribués et la technologie trop complexe. Les solutions d'inventaire automatisées avec agent ne permettent pas de fournir une transparence et visibilité ou même de récolter des données brutes d'une façon économique et en temps réel.

Face à ce besoin manifeste d'organisation, BDNA a investi du temps et des ressources considérables pour développer sa technologie d'inventaire, unique sur le marché.

Tout d'abord, BDNA Discover™ n'impose aucune contrainte au client pour débiter le processus d'inventaire. Cette solution n'utilise aucun agent logiciel, ne requiert l'ouverture d'aucun port spécifique et génère une activité réseau très basse. De la même façon, les divisions éloignées n'ont pas besoin de modifier leur mode de travail pour bénéficier des avantages de BDNA Discover™.

D'autre part, BDNA Discover™ utilise une méthodologie d'inventaire « scientifique » pour garantir sa précision. Cette solution est capable de trouver et d'identifier précisément les matériels et logiciels présentant des accès et des privilèges limités.

Enfin, la technologie d'inventaire de BDNA est rapide - capable d'inventorier des milliers d'actifs en quelques heures - contre des semaines et des mois requis par les solutions d'inventaire traditionnelles et plus limitées.

BDNA Discover™ fournit trois niveaux distincts d'inventaire:

- **L'inventaire Niveau 1** fournit une image, basée sur le réseau, instantanée et fidèle des actifs informatiques en ne nécessitant quasiment aucune intervention de la part de l'utilisateur.
- **L'inventaire Niveau 2** fournit le détail des actifs, y compris les logiciels installés, sans utiliser d'agent.
- **L'inventaire Niveau 3** fournit un inventaire détaillé des applications sans utiliser de logiciel d'inspection très lourd.

Chaque niveau d'inventaire est détaillé ci-dessous.

Inventaire Niveau 1

Description

L'inventaire Niveau 1 trouve et classe tous les actifs de l'entreprise basés sur TCP/IP ainsi que leurs services réseau associés. BDNA Discover™ identifie au minimum le type d'équipement, le système d'exploitation et les services réseau critiques installés sur le matériel. En outre, la solution peut souvent identifier la version, le modèle et les données du constructeur. Comme chaque actif a sa propre configuration, BDNA Discover™ fournira divers niveaux de détail sur les actifs inventoriés.

Un ordinateur pourra, par exemple, être classé « Solaris » ou « Cisco Switch » alors qu'un autre sera classé comme « Solaris, Version 5.8, Ultra-Enterprise » ou « Cisco Catalyst 2450, 12 cartes filles, mémoire 256MB ». Le niveau de détail découle de la configuration de chaque ordinateur. BDNA ne requiert l'installation d'aucun agent, la fourniture d'aucun protocole SNMP ou aucune modification de l'environnement configuré pour réunir cette information.

Préparation

BDNA Discover™ ne requiert que deux choses pour débiter l'inventaire niveau 1. La première, que les adresses IP cibles ou "réseau" soient entrées ou uploadées en masse dans BDNA. Les réseaux locaux sont de grands espaces du réseau global au sein d'une organisation et peuvent être aussi larges que des réseaux multiples de classe A ou aussi petits qu'une seule adresse IP. Normalement, les réseaux sont créés sur la base de groupements physiques ou logiques qui facilitent l'analyse. Par sa conception, BDNA Discover™ ne fait pas d'inventaire de réseau. Ceci découle du principe de conception qui veut

que la solution soit très peu intrusive ; en effet, l'inventaire informatique est une opération très agressive.

Deuxièmement, BDNA Discover™ a besoin d'un accès vers les actifs qu'il aura identifiés. Plus précisément, aucun filtre, contrôleur de trafic ou outils équivalents ne devraient être activés entre les serveurs de BDNA Discover™ et les actifs visés par l'inventaire. Dans le cas où BDNA Discover™ rencontrerait des barrières de sécurité définies, les adresses IP utilisées par BDNA devraient être autorisées par les pare-feu pour toute la durée du processus d'inventaire. La solution ne cherchera pas à franchir les systèmes de sécurité mais elle notera leur existence.

Lorsque les systèmes de sécurité interdisent l'accès à BDNA Discover™, un moteur distant de collecte de données pourra être déployé dans un modèle fédéré, faisant remonter l'information au serveur primaire de BDNA. Ces moteurs dédiés à la collecte communiquent avec les principaux serveurs de BDNA via le protocole SOAP dirigé vers les ports 80 ou 443. Dans cette situation, l'entreprise prend en charge la gestion de l'ordinateur distant en échange du maintien de la politique de sécurité appliquée par le pare-feu.

Exécution

BDNA Discover™ recherche et classe les actifs en interrogeant les machines et en analysant les résultats. Plus précisément, la solution envoie une série de paquets ICMP, TCP et UDP aux ordinateurs et en récupère les réponses. Elle nourrit le moteur d'inférence de BDNA Discover™ et celui-ci, à partir des réponses, en déduira le type de machine, le système d'exploitation et éventuellement d'autres données.

Pendant l'inventaire Niveau 1, BDNA Discover™ utilise de nombreux ports et protocoles reconnus. Au cours de l'analyse d'un ordinateur, BDNA Discover™ pourra utiliser jusqu'à huit protocoles différents pour identifier l'actif. La décision d'utiliser des protocoles supplémentaires est prise en fonction de la configuration de l'actif et du moteur d'inférence BDNA Discover™. Si la solution n'arrive pas à identifier un actif avec un protocole, elle renouvellera sa tentative avec d'autres.

Parallèlement, si elle a décelé un actif d'un certain type, elle pourra générer une demande spécifique afin de confirmer son inférence.

Suit une liste représentative de protocoles et de ports réseau utilisés par BDNA Discover™ :

- ICMP (ping)
- FTP (port 21);
- SSH (port 22);
- Telnet (port 23);
- SMTP (port 25);
- HTTP (ports 80, 443, 8080);
- POP2 (port 109);
- POP3 (port 110);
- NBT et d'autres protocoles Microsoft (ports 135-139)

SMB (port 445);
IMAP2 (port 143);
SNMP (port 161, UDP et TCP);
Serveur Microsoft SQL (port 1433);

Sécurité et Inventaire Niveau 1

Les principales objections concernant l'inventaire Niveau 1 portent sur la charge réseau générée et sur l'engorgement des accès. Tout d'abord, la solution BDNA Discover™ génère une charge réseau nominale. BDNA Discover™ utilise des techniques identiques aux scanners de sécurité mais ce n'est pas un scanner de sécurité. Les scanners de sécurité et ceux qui réalisent des cartographies réseau génèrent des charges beaucoup plus lourdes car leur but est d'analyser entièrement chaque port ouvert ou chaque connexion du réseau. La solution BDNA Discover™ génère seulement la quantité de trafic nécessaire à l'identification d'un actif, puis elle passe à l'actif suivant. En outre, elle peut aisément être limitée par le réseau et par protocole afin de réduire encore plus la charge réseau.

Ensuite, ses besoins d'accès réseau sont limités et ont été démontrés comme ayant une incidence proche de zéro sur les matériels existants. La solution BDNA Discover™ ne requiert pas d'accès réseau en continu. En revanche, elle peut opérer dans une fenêtre de temps suffisamment courte au cours de laquelle l'inventaire peut être étroitement géré. Ceci permet de minimiser le risque pendant ce laps de temps. De plus, BDNA Discover™ n'envoie pas de paquets IP malformés ou suspects à des ports inconnus ou sélectionnés au hasard, ce qui pourrait générer des résultats imprévisibles. Ceci garantit que BDNA Discover™ n'affectera pas les ordinateurs existants sur le réseau.

Résumé Niveau 1

L'inventaire Niveau 1 donne aux entreprises un aperçu rapide et complet de leur infrastructure informatique sans requérir un investissement en temps important. La FactBase générée par l'inventaire Niveau 1 permet au DSI de mettre en place des initiatives stratégiques telles que la rationalisation de sa force de vente, l'appui d'une fusion ou d'un désinvestissement, la gestion de la sous-traitance, voire plus.

Inventaire Niveau 2

Description

L'inventaire Niveau 2 fournit une information détaillée des logiciels et du système informatique. Plus précisément, BDNA Discover™ relève la configuration du système (nombre de processeurs, taille de la mémoire, type de machine, etc.), les numéros de série identifiables, les mémoires/disques durs externes connectés, la version du système d'exploitation, le niveau de patch du système, les patches installés, et plus encore. La solution vérifie également les attributs collectés au cours l'Inventaire Niveau 1 et fournit des détails supplémentaires si nécessaire.

BDNA Discover™ collecte également, au cours de cette phase d'inventaire, des informations sur les logiciels installés. BDNA développe et tient à jour une base d'« empreintes » des principaux logiciels rencontrés. Les efforts de développement sont axés sur des logiciels critiques tels que des bases de données, des serveurs d'application ou des applications qui présentent de fortes opportunités de réduction de coûts ou de risques.

Préparation

Afin de mettre en œuvre la collecte Niveau 2, BDNA Discover™ requiert un certificat pour accéder au matériel inventorié. Ce certificat est en règle générale le nom d'un utilisateur du système d'exploitation et un mot de passe pour accéder au serveur ou à l'ordinateur (Unix ou Windows) mais peut également être une communauté SNMP privée s'il s'agit d'un commutateur réseau ou d'un routeur. Le certificat ne requiert pas de « root » ni d'autre niveau d'accès d'administrateur. BDNA Discover™ est capable d'utiliser des comptes à privilège d'accès normal car elle ne tente pas de modifier ou de gérer l'ordinateur en cours d'inventaire ; le but étant simplement d'évaluer la machine.

Pour les systèmes sous Unix, BDNA Discover™ est en mesure de reconnaître une large variété de méthodes de connexion y compris SSH, telnet, rsh et SNMP. Afin de faciliter la gestion des déploiements de grande ampleur, BDNA recommande l'utilisation de SSH avec des clés publiques/privées, ce qui facilitera l'accès.

Pour les systèmes sous Windows, BDNA Discover™ utilise le protocole WMI (Windows Management Instrumentation). L'inventaire en WMI n'a pas besoin pour fonctionner d'un compte Windows administrateur, avec les privilèges WMI afférents. Dans le cas d'un déploiement, BDNA recommande de créer un compte au niveau du domaine avec les privilèges WMI appropriés.

Les certificats pourront être utilisés pour rechercher des ordinateurs à divers degrés de finesse. Par exemple, un certificat pourrait être utilisé pour un seul système sous Unix ou pour tous les systèmes sous Unix d'un même réseau. S'il existe plusieurs certificats pour un seul ordinateur, BDNA Discover™ essaiera chaque certificat à tour de rôle jusqu'à ce qu'il trouve celui qui marche et que la connexion puisse se faire.

Exécution

Le processus de collecte Niveau 2 couvre la connexion au système inventorié et la collecte des données. La technique utilisée pour la collecte varie selon le système d'exploitation. BDNA Discover™ utilise des techniques allant des shell scripts au WMI. Indépendamment de la méthode de collecte, la solution n'augmente pas la charge du système à inventorier. De plus, de même que pour la collecte Niveau 1, la collecte Niveau 2 peut être limitée par protocole et réseau.

Au cours de la recherche de logiciels, BDNA Discover™ recherche des processus et des signatures indiquant quels logiciels sont installés. Bien qu'un certain nombre d'attributs soient collectés pour tous les logiciels, lieu d'installation et version par exemple, BDNA

Discover™ peut collecter d'autres attributs pertinents en fonction du type du logiciel découvert. Ceci peut inclure des données de licence, dates d'installation, voire plus.

Sécurité et Inventaire Niveau 2

Les objections concernant le Niveau 2 portent sur la consolidation des certificats. Le risque est modéré par trois facteurs importants. Tout d'abord, BDNA Discover™ n'a aucun besoin de certificats d'administrateur. Il a juste besoin de certificats pour des utilisateurs de comptes standards dont les droits sont typiquement limités par les systèmes individuels. D'autre part, sur les systèmes sous Unix, BDNA Discover™ peut utiliser le protocole SSH, par nature plus sûr. Ce risque est encore réduit si l'on utilise des clés publiques/ privées au lieu de mots de passe. Enfin, sur les équipements sous Windows, des systèmes de collecte séparés peuvent utiliser des sous-ensembles de certificats de façon à ce que ni le référentiel de BDNA Discover™ ni aucun autre système ne puisse être en possession de l'ensemble des certificats pour tous les équipements sous Windows.

Résumé Niveau 2

L'inventaire Niveau 2 fournit aux entreprises un inventaire précis de leur parc informatique et une information riche sur les éléments inventoriés, ainsi que sur leurs systèmes critiques sans avoir à déployer d'agent.

L'inventaire Niveau 2 vient en appui des décisions et des activités stratégiques des Opérations Informatiques et des Achats telles que la renégociation de la force de vente et la consolidation des serveurs et du stockage.

Inventaire Niveau 3

Description

L'inventaire Niveau 3 fournit un inventaire détaillé des applications spécifiques. Il recherche les installations d'applications et les instances actives pour en extraire l'information pertinente pour la gestion des actifs tels que les comptes utilisateurs, l'utilisation de la mémoire ainsi que d'autres données d'applications spécifiques. De même que pour l'inventaire Niveau 2, BDNA développe et tient à jour une base d'« empreintes » pour bases de données et applications. La distinction entre le Niveau 2 et le Niveau 3 est l'obligation de fournir un certificat supplémentaire spécifique par application.

Préparation

Afin de mettre en œuvre l'inventaire Niveau 3, BDNA Discover™ requiert un certificat spécifique à l'application. On considèrera l'exemple d'une entreprise voulant utiliser BDNA afin de trouver des informations plus précises que celles fournies par le Niveau 2 (liste d'installations, versions et instances actives) pour ses utilisations de la base de données Oracle. Cet inventaire requiert un certificat d'utilisateur de la base Oracle. De même que pour le Niveau 2, ce certificat n'a pas besoin de privilèges d'administrateur mais il requiert un accès en lecture aux structures d'application appropriées (les tables de base de données Oracle dans ce cas précis) afin de collecter les données. BDNA Discover™ fournit les outils

nécessaires pour créer ces comptes d'application à accès spécifique. De plus, pour mettre en œuvre l'inventaire Niveau 3 sur une application spécifique, BDNA Discover™ doit avoir mis en œuvre l'analyse Niveau 2 sur l'actif où l'application est installée.

Exécution

Le processus de collecte Niveau 3 consiste en une connexion au système utilisant la méthode définie et utilisée par l'inventaire Niveau 2 puis en l'exécution de scripts ou de programmes supplémentaires destinés à collecter les données. Sur les bases de données Oracle par exemple, BDNA Discover™ exécutera la ligne de commande SQL*Plus dans l'interface de commande SQL, pour extraire les données. Le logiciel d'« empreintes » Niveau 3 de BDNA Discover™ gère le processus total de connexion et de collecte sans aucune intervention manuelle. Les attributs collectés varient selon le type d'application découverte. En ce qui concerne les bases de données, BDNA Discover™ pourra collecter un maximum d'information sur la mémoire et son allocation. Pour les progiciels de gestion intégrés, la solution collectera les données sur les modules installés et leur utilisation.

Indépendamment du type d'application, BDNA Discover™ collecte les attributs qui présentent un intérêt au niveau général ou pour un système en particulier. Cependant, il est à noter que, bien que les caractéristiques opérationnelles soient facilement inventoriées, BDNA n'a pas pour objectif de les gérer.

Sécurité et Inventaire Niveau 3

Les objections concernant le Niveau 3 sont principalement associées aux données collectées par BDNA Discover™. En particulier, lorsqu'on lui autorise l'accès aux bases de données ou aux installations des progiciels de gestion, émergent des soucis évidents de confidentialité et de légalité. Cependant, BDNA Discover™ ne peut en aucun cas mettre en œuvre une quelconque collecte sans une autorisation explicite. Par conséquent, le compte d'application fourni à BDNA Discover™ doit pouvoir contrôler le niveau d'accès. A partir du moment où le compte utilisateur de l'application requis par BDNA Discover™ est ciblé et limité, les données collectées seront également ciblées et limitées.

Résumé Niveau 3

L'inventaire Niveau 3 fournit aux entreprises des données applicatives spécifiques sans installation ou utilisation d'agents. Par l'inventaire Niveau 3, le DSI aura la transparence nécessaire pour appuyer des activités telles que la renégociation de la force de vente, la rationalisation des applications, les audits internes et la refacturation.

Résumé

BDNA Discover™ crée un état complet et fiable de tous les actifs en fournissant la transparence et le détail nécessaires à la mesure et à la gestion d'une organisation informatique. La solution permet aux organisations informatiques de connaître rapidement ce qu'elles ont, ce qu'elles utilisent et ce dont elles ont réellement besoin. La méthodologie d'inventaire à trois niveaux de BDNA utilise des techniques simples et bien connues pour

fournir une information très fiable instantanée et répétitive. Les résultats de l'inventaire fournissent aux preneurs de décisions l'information nécessaire pour entamer le processus d'élimination des déchets informatiques.

Au sujet de BDNA

BDNA est l'entreprise du Génome Informatique™.

BDNA (www.bdna.com) a passé une dizaine d'années à cartographier le Génome de la Technologie de l'Information. Le résultat en est Technopedia™ - la première encyclopédie du Génome informatique, un recensement complet de l'information critique sur tous les principaux produits software et hardware de l'industrie technologique. Le centre BDNA du Génome Informatique, construit autour de Technopedia™, permet aux entreprises informatiques de séquencer leur propre ADN pour enfin Savoir Ce Dont Ils Sont Faits (Know What They Are Made Of™), et éliminer les déchets informatiques. La base de clients de BDNA comprend HSBC, Lockheed Martin, Motorola, Pfizer, l'Etat de Californie, Telecom Italia, AstraZeneca, US Army et la Banque Mondiale. BDNA est basée à Mountain View en Californie, et elle possède des bureaux de vente sur tout le continent Nord Américain, en Europe et en Asie.

Pour plus d'informations, veuillez vous rendre sur le site theitgenome.com.

Siège social – Etats-Unis

339 North Bernardo Avenue, Suite 206
Mountain View, CA 94043
T: 001(650) 625-9530
F: 001(650) 625-9533
americasales@bdna.com

Côte Est des Etats-Unis

Georgetown Place
1054 31st Street NW, Suite 300
Washington, DC 20007
T: 001(202) 595-7751
F: 001(202) 625-8376

Europe

121-123 Rue Edouard Vaillant
92300 Levallois-Perret
France
T: +33 (0)1 41 27 65 42
F: +33 - (0)1 41 27 65 57
internationalsales@bdna.com

Asie-Pacifique

202 West Tower, JiaDu Building
64-66 JianZhong Road
TianHe District
Guangzhou
GuangDong Province
China
T: +8620 - 856 13650