

SYSTEMES D'INFORMATION DE LA BIBLIOTHEQUE NATIONALE DE FRANCE

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

ANNEXES B4 DOSSIER DE SYNTHESE DE L'ARCHITECTURE DES SYSTEMES D'INFORMATION

LA SUPERVISION

TABLE DES MATIERES

1. INTRODUCTION	3
1.1 OBJECTIFS DE LA SUPERVISION	3
1.2 LES COMPOSANTS SUPERVISES	3
1.3 UTILISATION DE LA SOLUTION DE SUPERVISION.....	4
2. DESCRIPTION DE L'EXISTANT EN TERME DE SUPERVISION	5
2.1 LA SOLUTION DE SUPERVISION DU SYSTEME D'INFORMATION	5
2.2 MAINTENANCE DE LA SOLUTION ACTUELLE	6
2.3 LA SUPERVISION RESEAU	6
2.4 LA SUPERVISION SYSTEME.....	7
2.5 LA SUPERVISION APPLICATIVE.....	8
2.6 L'HYPERVERSION	8
2.6.1 <i>Présentation générale d'Alerta</i>	8
2.6.1.1 Présentation de l'interface web	9
2.6.2 <i>Description réception des données dans Alerta à la BnF</i>	9
2.6.2.1 Bases.....	9
2.6.2.2 Fonctionnement	9
2.6.3 <i>Exemple de vue des alertes</i>	9
3. LA SUPERVISION DES SERVICES WEBS EXTERNES	11
4. LE REFERENTIEL DE SUPERVISION.....	12

1. INTRODUCTION

1.1 OBJECTIFS DE LA SUPERVISION

Le système de supervision du Système d'Information de la BnF a pour rôle de permettre, d'une manière générale, de :

- Garantir la disponibilité du système d'information ;
- maintenir le système d'information en conditions opérationnelles ;
- maîtriser et optimiser le fonctionnement du système d'information ;
- analyser et déterminer la cause des incidents ;
- mesurer la charges et les performances des ressources afin d'améliorer la qualité de service aux utilisateurs ;
- maîtriser les évolutions.

Pour que ces objectifs puissent être atteints de manière efficace, il est nécessaire de fédérer au sein d'une solution de supervision offrant :

- des fonctions de supervision du système d'information, s'appuyant sur une plate-forme centrale,
- des visions détaillées par domaine technique,
- des fonctions d'administration fines par domaine technique, éventuellement basées sur des outils spécifiques mais accessibles à partir de la plate-forme centrale de supervision.

Ceci en tenant compte des quatre composantes essentielles :

- les objets ou composants techniques,
- les domaines techniques,
- les fonctions,
- les acteurs.

1.2 LES COMPOSANTS SUPERVISES

Les différents domaines techniques supportés par la supervision sont :

- Le réseau (LAN, WAN),
- Les systèmes (Windows, UNIX),
- Les services (middleware, SGBD, webs...)
- Les applications.

1.3 UTILISATION DE LA SOLUTION DE SUPERVISION

Le tableau suivant présente les différents profils d'utilisateurs de la solution de supervision.

Fonction	Appartenance	Niveau de support	Tâches liées à l'outil de supervision
Superviseur	Infogérant	Niveau 1	➤ Surveillance permanente de l'état du SI (cartographie et alarmes temps réel) ➤ Mises à jour (cartographie, alarmes...) liés à l'ajout d'un nouvel équipement dans le périmètre de la supervision ➤ Installation et paramétrage des agents de supervision
Administrateur d'un domaine technique	BnF/DSI	Niveau 2	➤ Analyse de deuxième niveau des incidents (en utilisant conjointement des outils spécialisés hors supervision)
Administrateur des serveurs et logiciels de supervision	BnF/DSI	Niveau 2	➤ Assurer le bon fonctionnement matériel et logiciel de la plate-forme ➤ Gérer les évolutions et effectuer les mises à jour importantes ➤ Assurer le support technique sur la solution pour les superviseurs

2. DESCRIPTION DE L'EXISTANT EN TERME DE SUPERVISION

2.1 LA SOLUTION DE SUPERVISION DU SYSTEME D'INFORMATION

La solution de supervision de la BnF permet de traiter des événements en provenance de l'ensemble du système d'information (réseaux, systèmes, services, applications).

Elle est composée principalement des logiciels :

- **Alerta** : Logiciel de centralisation des alertes des différentes sources
- **Nagios** : Logiciel de supervision Opensource
- HP : **Openview Network node manager**

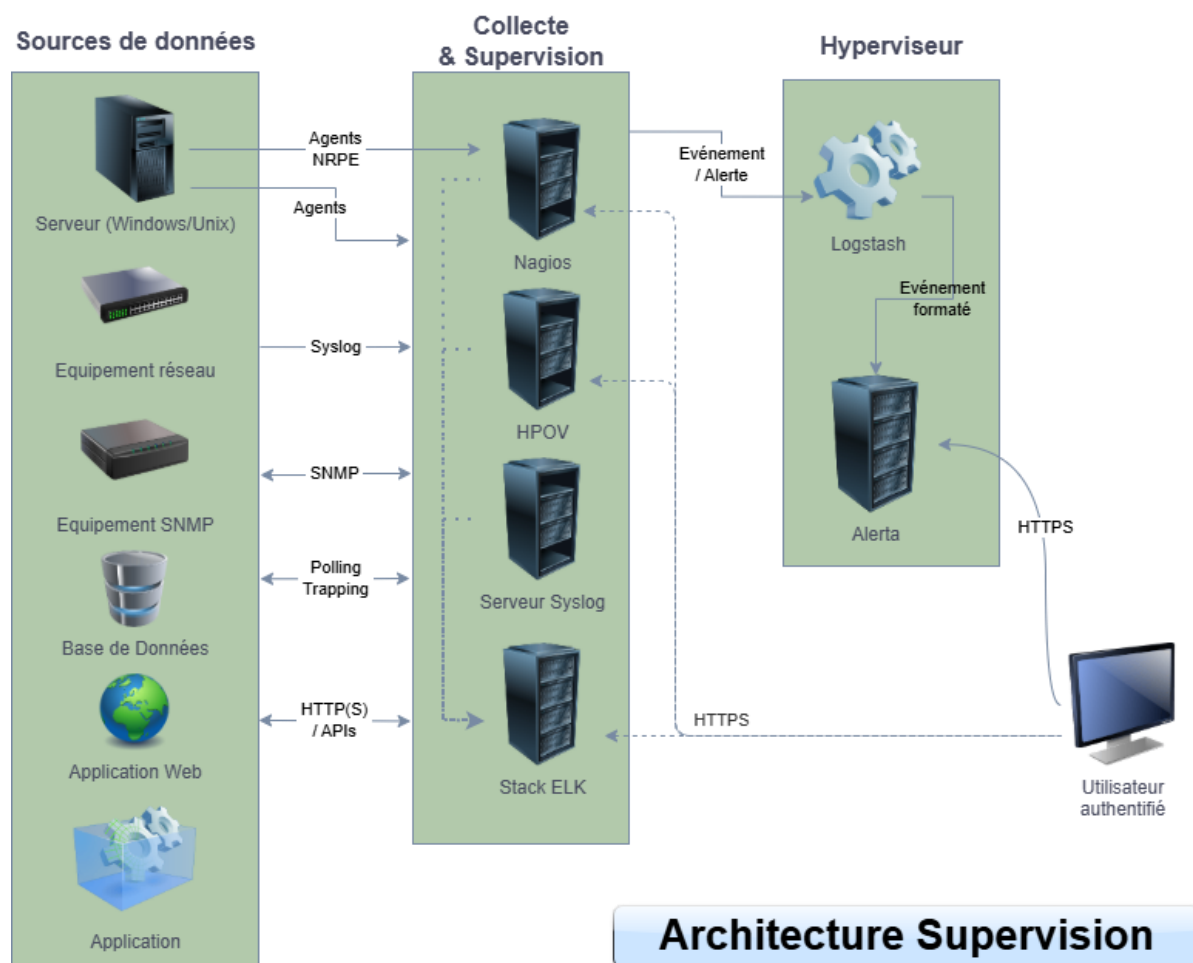
La fonction d'**hypervision** est assurée par le composant **Alerta**.

Les événements (alarmes ou informations) sont collectés via :

- SNMP (traps principalement) depuis les agents SNMP natifs des équipements ou depuis des agents SNMP installés sur les serveurs à superviser,
- Syslog,
- NRPE : protocole utilisé par Nagios pour la communication avec les agents installés sur les serveurs Windows/Unix.

Ces événements sont traités (filtrés, corrélés, reformulés...) pour ensuite être présentés dans l'interface utilisateur.

L'architecture



Les logiciels

Le tableau ci-après présente la liste des modules logiciels de la solution actuelle

Module	Editeur	Serveurs
Alerta	Alerta	Serveur alerta
Logstash	Stack Elastic	Serveur alerta
Nagios Nagios-core (base)	Nagios	Serveur nagios
Nagios plugins	-	Serveur nagios
Cacti	-	Serveur cacti
Syslog-ng	-	Serveur cacti et nagios
nsclient	-	Serveur windows à superviser
Nagios NRPE	-	Serveur Linux à superviser

Serveur	Système d'exploitation
Nagios	Linux CentOS
Cacti	Linux CentOS
HP Openview	Linux RedHat
Alerta	Linux Almalinux

2.2 MAINTENANCE DE LA SOLUTION ACTUELLE

Le logiciel HP Openview est sous maintenance renouvelable d'année en année.
Les autres logiciels (open source) ne sont pas sous maintenance.

2.3 LA SUPERVISION RESEAU

La supervision du réseau est assurée principalement par le logiciel HP OpenView NNM (network node manager) version 9.10.

Cette supervision est basée essentiellement sur **le protocole SNMP**.
Certains éléments sont également supervisés via le protocole **syslog**.

Les événements pouvant apparaître sur la plate-forme HP OpenView sont de trois types :

- les alarmes associées à des changements d'états : nœud réseau qui ne répond plus, interface down,
- les alarmes de dépassement de seuils sur des indicateurs de surveillance et de charge du réseau. Ces seuils sont calculés à partir des indicateurs fournis par la MIB des équipements réseaux.
- les traps SNMP renvoyés par les équipements réseaux.

Pour pouvoir superviser le réseau de manière optimale, les MIB des équipements doivent être compilées dans HP Openview (à partir du fichier MIB texte au format ASN1). L'ensemble des MIB cisco a donc été compilé et intégré à HP Openview à la BnF

A titre indicatif voici des exemples de collectes SNMP utilisées pour les dépassement de seuil :

Anomalies	
Interfaces (niveau 2)	• Dépassement de seuil de l'utilisation de la bande passante en pourcent (If%util)
	• Dépassement de seuil du taux de paquets en erreur en entrée en pourcent (IfInPktPctErrors)
	• Dépassement de seuil du taux de paquets en erreur en sortie en pourcent (IfOutPktPctErrors)
	• Dépassement de seuil du nombre de paquets broadcast par seconde (BroadcastPkts)
Routage	• Dépassement de seuil de Problème de routage / S (RoutErrors)
Activité système	<u>Activité CPU</u> • Dépassement de seuil du taux CPU sur 5 minutes (cpmCPUTotal5minRev)
	<u>Activité mémoire</u> Dépassement de seuil du taux d'occupation de la mémoire en pourcentage (MemoryUsed)
Trafic Niveau 3	• Trafic sur le vlan

Le système de cartographie est de type hiérarchisé ou arborescent et permet ainsi de passer d'une vue générale à des vues détaillées. La découverte d'un équipement IP se fait automatiquement par un service qui explore le réseau.

La BnF utilise le logiciel opensource **Cacti** pour collecter le trafic et les erreurs sur les ports des switchs réseaux et pour représenter ces collectes sous la forme de tableaux de bord.

2.4 LA SUPERVISION SYSTEME

La supervision système concerne les systèmes d'exploitations figurant dans le tableau ci-dessous. Le protocole nrpe (nagios ou nsclient) est le plus utilisé. Le protocole syslog est utilisé en cas de besoins dans des cas particuliers.

Systèmes	Versions (actuelles à titre indicatif)	Agent ou module
Windows	2008, 2012, 2019, 2022	Nsclient en mode nrpe
Linux	Almalinux (9,10), CentOS (7,8,9), Redhat / Debian	Nagios nrpe Syslog

Ci-dessous, sont regroupés les principaux domaines de la supervision système. Pour certains cas particuliers, des plugins ou scripts spécifiques, qui n'apparaissent pas dans ce tableau, ont été développés. Il existe des valeurs seuils génériques (par système, par fonctionnalité...) ou spécifiques.

Domaine	Système	Type de surveillance
CPU	Unix / Windows	Dépassement de seuil
Mémoire	Unix / Windows	Dépassement de seuil
Mémoire virtuelle	Unix / Windows	Dépassement de seuil
Espace disque	Unix / Windows	Dépassement de seuil
Redémarrage	Unix / Windows	Date de redémarrage

Domaine	Système	Type de surveillance
Services de sauvegarde	Unix / Windows	Présence service et process
Journal applicatif	Windows	Parsing de log
Journal Système	Windows	Parsing de log
Services Antivirus	Windows	Présence service et process
Services spécifiques windows	Windows	Présence service et process
Load average	Unix	Dépassement de seuil
Services spécifiques unix	Unix	Présence process
Journal système (messages)	Unix	Parsing de log

2.5 LA SUPERVISION APPLICATIVE

La supervision applicative est basée soit sur une vérification de paramètres de fonctionnement (logs, présence d'un process...) soit par simulation d'un accès utilisateur (requête http vers serveurs webs, ...).

Domaine	Système	Type de surveillance
Journal applicatif	Unix / Windows	Parsing de log
Service applicatif	Unix / Windows	Présence service et/ou process
Service web	Unix / Windows	Requête http
Service dns	Unix / Windows	Requête dns
Service ftp	Unix / Windows	Requête ftp
Service normalisé	Unix / Windows	Requête protocolaire
Base de donnée	Unix / Windows	Requête base de donnée
Application spécifique	Unix / Windows	Plugin (script) spécifique

2.6 L'HYPERVISION

L'hypervision permet la collecte et le traitement centralisé de l'ensemble des informations de supervision (réseaux, systèmes, applications). Ces informations sont traitées (filtrage, corrélation, déduplication...) et affichées dans l'interface utilisateur.

La collecte est effectuée par nagios, syslog et openview. Les événements sont injectés après traitement (déduplication, filtrage, reformulation, etc...) dans la base de données de l'hyperviseur.

L'interface utilisateur affiche les événements récupérés des différentes sources.

Il est par exemple possible de visualiser sous forme d'une liste l'ensemble des événements liés à un serveur ou à une application. Ces listes peuvent être triées ou filtrées pour ne voir par exemple que les événements critiques.

2.6.1 Présentation générale d'Alerta

Alerta est un produit Opensource qui sert à superviser l'infrastructure informatique de la BnF.

Il fournit une interface web permettant l'hypervision de l'infrastructure.

2.6.1.1 Présentation de l'interface web

L'interface web affiche une liste des alertes, pouvant être filtrées par état (alertes en cours, nouvelles, mises de côté...), par groupes (http, système, logs, bases de données...), par environnement...

2.6.2 Description réception des données dans Alerta à la BnF

2.6.2.1 Bases

Le logiciel Logstash est utilisé pour réceptionner tous les événements des différentes sources (Nagios...).
Chaque DataSource a des règles qui lui sont associées.
Le langage utilisé est propre à Logstash.

2.6.2.2 Fonctionnement

Lors de la réception d'un événement un traitement est déclenché suivant la dataSource et se chargera des remaniements, formatages et filtres qui lui sont appliqués et va générer l'Identifiant de l'alerte potentielle avant de l'enregistrer dans Alerta.

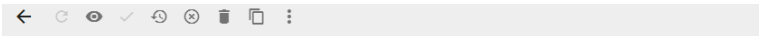
Si cet identifiant existe déjà et que l'évènement n'est pas en état d'alerte, alors l'alerte en question sera clôturée.

2.6.3 Exemple de vue des alertes

The screenshot shows the Alerta web interface. At the top, there's a search bar and a navigation menu. Below the navigation menu, there's a summary table with counts for different alert states:

EN COURS				NOUVELLES				PRISES EN COMPTE				MISES DE COTE			
0	2	34	0	0	2	34	0	0	0	0	0	0	8	114	26

Below the summary table, there's a table of alerts. The table has columns for Statut, Dernière réception, Doublons, Environnement, Ressource, Service, and Description. The first few rows show alerts with status 'Open' and 'ven, 29 mai 14:47'.



DÉTAIL

Id alerte	dcc2cf87-9269-4a11-bb6e-781cfe5eb929
Dernier Id reçu	342d1d2a-6862-4d6a-a437-3618d87f8d34
Date de création	ven. 22 mai, 2026 18:00:19.950 +02:00 (il y a 7 jours)
Date de réception	ven. 22 mai, 2026 18:00:19.958 +02:00 (il y a 7 jours)
Dernière réception	ven. 29 mai, 2026 14:58:57.284 +02:00 (il y a 2 minutes)
Service	Utilisation FileSystems
Environnement	PFO
Ressource	
Evènement	UtilisationFileSystemsvar
Corrélation	
Groupe	Charges
Gravité	Normal → Major
Statut	Shelved par alerta_ingest (il y a 2 minutes)
	🕒 free space: /var 839M (4%)
Valeur	free space: /var 839M (4%)
Texte	free space: /var 839M (4%)
Indicateur Trend	More Severe
Délai	259200
Type	SERVICEALERT
Doublons	3429
Répéter	True
Origine	nagios:
Tags	MZ PFO En service
Env	PFO
Etat	En service
Hostname	
Libelle	Serveur
Nagios_Service	Utilisation FileSystems
Zone	MZ

3. LA SUPERVISION DES SERVICES WEBS EXTERNES

La BnF utilise **IP-Label** pour mesurer la **qualité de services de ces principaux services web externes**.

Il s'agit d'une solution en mode ASP (Application service provider), hébergée par Ekara, et paramétrable et consultable par le ou les administrateurs BnF des sites.

IP-Label permet de répondre à deux types principaux de besoins :

- la mesure de la disponibilité et des performances des transactions réalisées par les internautes lors de leur parcours sur le site ;
- le suivi des mesures de la qualité d'accès aux sites perçue par les internautes.

Hormis la consultation directe au travers d'un navigateur web, IP-Label permet de paramétrer des alertes envoyées par courrier électronique.

Deux types d'alertes sont remontés en fonction d'un dysfonctionnement total ou partiel.

Différents type d'éléments sont mesurés :

- la disponibilité des sites,
- le temps d'accès aux sites,
- les temps d'accès des différents objets (images, sons,...) composant la page auditée,
- le temps de réalisation d'une « transaction » utilisateur.

Une transaction utilisateur est définie comme un ensemble d'actions séquencées effectuées par l'utilisateur lors de la consultation d'un site BnF. Ces transactions sont regroupées en scénarios de tests.

La BnF dispose au total de 12 scénarios de tests.

Ces **scénarios sont exécutés par des robots**.

Bibliothèque nationale de France	Cahier des Clauses Techniques Particulières
	Annexe B4 - Dossier de synthèse de l'architecture des Systèmes d'Information La Supervision

4. LE REFERENTIEL DE SUPERVISION

Il contient notamment pour chaque serveur :

- Le nom du serveur,
- Le type d'OS,
- Le groupe fonctionnel du serveur,
- La fonction du serveur,
- La liste synthétique des applications sur le serveur,
- La zone du serveur,
- Les process/services spécifiques supervisés,
- Les logs spécifiques supervisés,
- Les surveillances basiques (Utilisation CPU, disque, mémoire...)
- Les surveillances spécifiques,
- etc...