Syslog : présentation

Le protocole Syslog est défini dans la RFC 3164.

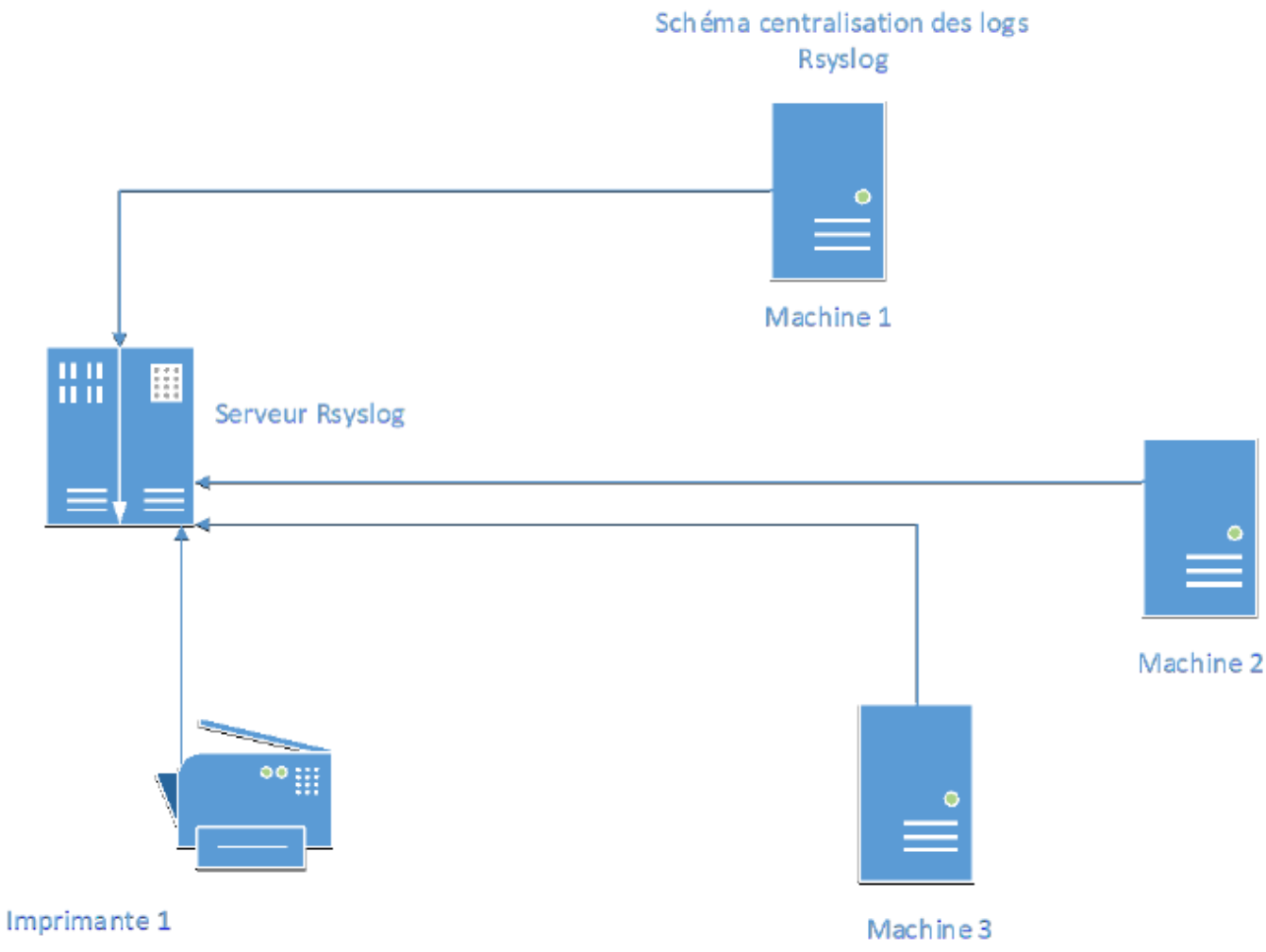
Les messages syslog générés par les équipements réseaux et les serveurs peuvent être envoyés vers des collecteurs de messages d'événements ou serveurs Syslog.

Les messages sont envoyés avec le protocole UDP (User Datagram Protocol) sur le port 514.

Depuis 2004, le projet RSyslog a été développé en OpenSource en utilisant le port UDP 514 mais aussi le port TCP 10514.

Attention : le port TCP 514 peut également être utilisé par le service RPC.

Principes de fonctionnement du protocole syslog



Les logs contiennent un ensemble de données d'informations générés par un système d'exploitation ou un équipement réseau.

Afin de faciliter le travail des administrateurs, Syslog permet de centraliser tous les messages générés par différent serveur et équipements du réseau vers une seule machine qui servira de serveur de log.

La version RSyslog permet la centralisation des logs et apporte de nouvelles fonctionnalités par rapport à Syslog. Cette version est la plus utilisée sur les plateformes. Elle permet aussi, via un client spécifique, de gérer des machines clientes sous Windows.

La suite de ce document sera basée sur RSyslog.

Le protocole fonctionne en utilisant le modèle client/serveur :

- Le serveur va centraliser tous les messages de logs envoyés par les clients
- Les messages sont normalisés et contiennent notamment les adresses IP, la criticité de l'événement, les messages liés à l'événement, l'horodatage de l'événement, etc.

Les journaux de logs sont classés par thèmes :

Thèmes	Définition
auth	Utilisé pour des évènements concernant la sécurité ou l'authentification à travers des applications d'accès (type SSH)
authpriv	Utilisé pour les messages relatifs au contrôle d'accès
daemon	Utilisé par les différents processus systèmes et d'application
kern	Utilisé pour les messages concernant le noyau (kernel)
mail	Utilisé pour les évènements des services mail
user	Par défaut quand aucun n'est spécifié
local7	Utilisé pour les messages du boot
*	Désigne tous les éléments

Les niveaux de log

Log level	Signification
Emerg	Situation de panique
Alert	Situations urgentes
Crit	Situation système critique
Err	Autre erreur
Warning	Avertissement
Notice	Évènements normaux devant être signalés
Info	pour information
Debug	message de débogage

La centralisation de tous les messages en utilisant le même format permet une exploitation simplifiée des données. La gestion des journaux d'évènements est un complète la supervision sans la remplacer.

La supervision est effectuée en temps réel alors que dans la majorité des cas le travail avec les journaux se fait à postériori. Mais ce travail à postériori est indispensable pour analyser les problèmes **à froid** et permettre d'en tirer les conséquences et donc d'éviter au maximum que l'incident se réitère.