

Formation scribe

Nicolas Poulain - Dafor 2012

19 mars 2012

Table des matières

1 Les modules EOLE	1
1.1 Scribe : Un serveur pédagogique complet.	2
1.2 Schéma d'un réseau d'établissement	2
1.3 Déroulement de la formation	2
2 Mise en place du serveur	5
2.1 Installation	5
2.1.1 Configuration scribe 2.2	6
2.1.2 Configuration scribe 2.3	6
2.1.3 Instanciation	6

1 Les modules EOLE

Extrait de <http://eole.orion.education.fr/index.php/home>



FIGURE 1 – Logo EOLE

Eole est un projet collaboratif basée sur la philosophie du logiciel libre. La mutualisation des compétences et des moyens permet de réaliser des solutions économiques, fiables et performantes.

Chaque module constitue une distribution GNU/LINUX spécifique qui permet d'installer facilement un serveur dédié. Les services offerts sont pré-configurés, l'ensemble est cohérent. Vous devez télécharger sur ce site l'image ISO qui vous permettra de graver un DVD ou un CD d'installation. Ce DVD/CD est multi module, le choix du module à installer est proposé au démarrage (boot).

Les modules sont disponibles en deux versions

EoleNg 2.3	EoleNg 2.2
- Disponible depuis le 16 Janvier 2009.	- Disponible depuis le 8 Juin 2011.
- basée sur la version 8.04 Ubuntu	- basée sur la version 10.04 Ubuntu
- Arrêt du support mises à jour : Juin 2013	- Arrêt du support mises à jour : Juin 2015

1.1 Scribe : Un serveur pédagogique complet.

Scribe est un contrôleur de domaine dotée de fonctions évoluées. Il optimise la gestion de votre parc de stations clientes. Il dispose d'un annuaire qui référence, élèves, parents, personnels enseignant et administratifs, il propose un service de messagerie et héberge vos applications web au sein d'un portail Web 2.0.

Scribe est un contrôleur de domaine.

- gestion des connexions réseau des utilisateurs ;
- partage de fichiers et de répertoires ;
- support des ACL ;
- partage d'imprimantes ;
- gestion des comptes utilisateurs et des accès ;
- exécution d'applications utilisateurs ;

Scribe est un système de messagerie articulé autour d'un annuaire performant.

- l'annuaire est initialisé à partir d'importation de comptes (SCONET, BE1D, AAF, CSV,...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseaux ;
- la messagerie gère deux domaines distincts (l'Internet et l'intranet académique) ;
- utilisation au choix d'une interface web multilingue ou d'un client de messagerie standards.
- un service de listes de diffusion ;
- une sécurité antispam, un antivirus, une gestion de quotas (taille des boîtes aux lettres)

Scribe offre des services web =>Envole2.0

- un serveur web ;
- un portail web ;
- des applications pré-installés

Scribe est un serveur d'authentification unique (SSO)

- Eole SSO Utilise l'annuaire LDAP
- Les standards C.A.S 2 et OpenID sont supportés
- La fédération d'identité est possible via le protocole SAML.

Scribe dispose d'une gestion avancée des utilisateurs et des postes clients

- Distribution de devoir
- Contrôle d'accès à Internet et aux services réseaux
- appliquer des restrictions ou préconfigurer des applications, en fonction du login de l'utilisateur ou de ses groupes et du nom de la machine sur laquelle il se connecte ;
- effectuer des actions distantes sur les stations (fermer la session, éteindre ou redémarrer un ou plusieurs postes) ;
- surveiller la détection de virus par le serveur ;

1.2 Schéma d'un réseau d'établissement

Sur l'académie de Paris, les réseaux d'établissement sont organisés par la DSI, service informatique du Rectorat qui assure en plus l'administration et la maintenance des serveurs Amon, Scribe et Horus. Voir figure 2.

Les établissements assurent par eux-même les tâches de gestion courante du réseau et des machines avec les droits qui leur sont laissés en utilisant au travers des interfaces de gestion de ces serveurs.

1.3 Déroulement de la formation

Durant cette formation, nous allons simuler un réseau d'établissement grâce à des machines virtuelles. Cela nous permettra de contrôler complètement tous les éléments, d'effectuer tous les tests sans risque pour les machines réelles et le réseau qui nous entourent.

Sur la figure suivante, on simule plusieurs machines sur une seule appelée machine hôte. Un poste windows virtuel est un ordinateur virtuel sur lequel a été installé un système d'exploitation comme on le fait sur une machine réelle.

La situation décrite sur la figure 3 est équivalente à celle de la figure 4.

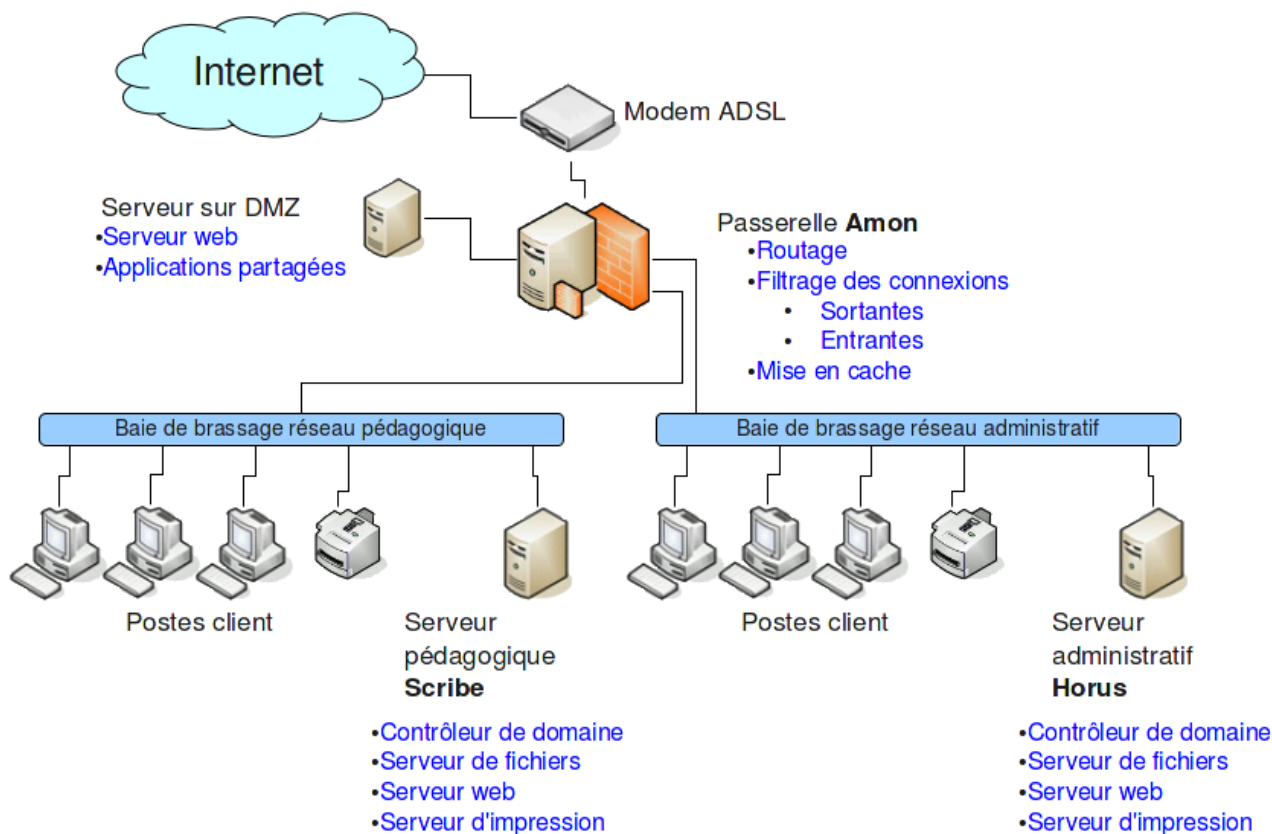


FIGURE 2 –

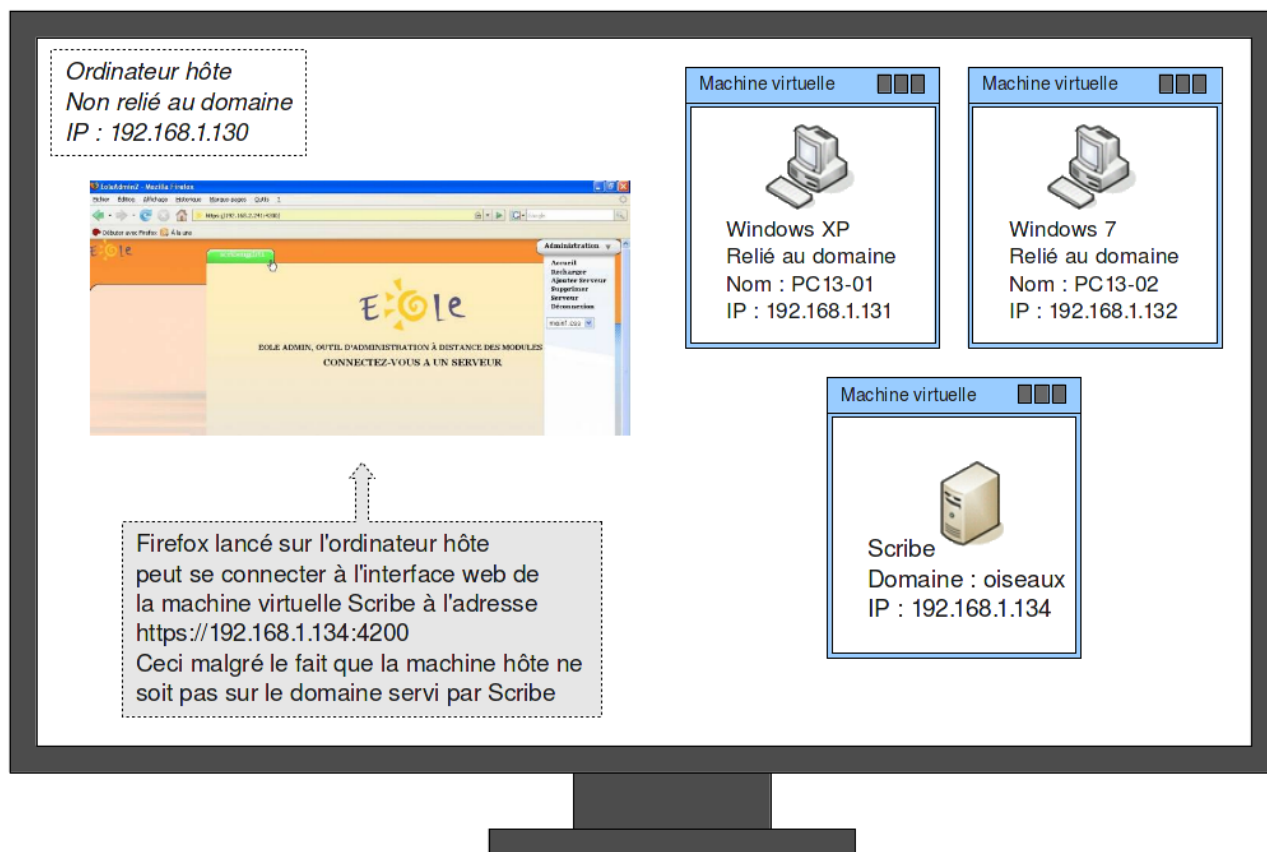


FIGURE 3 –

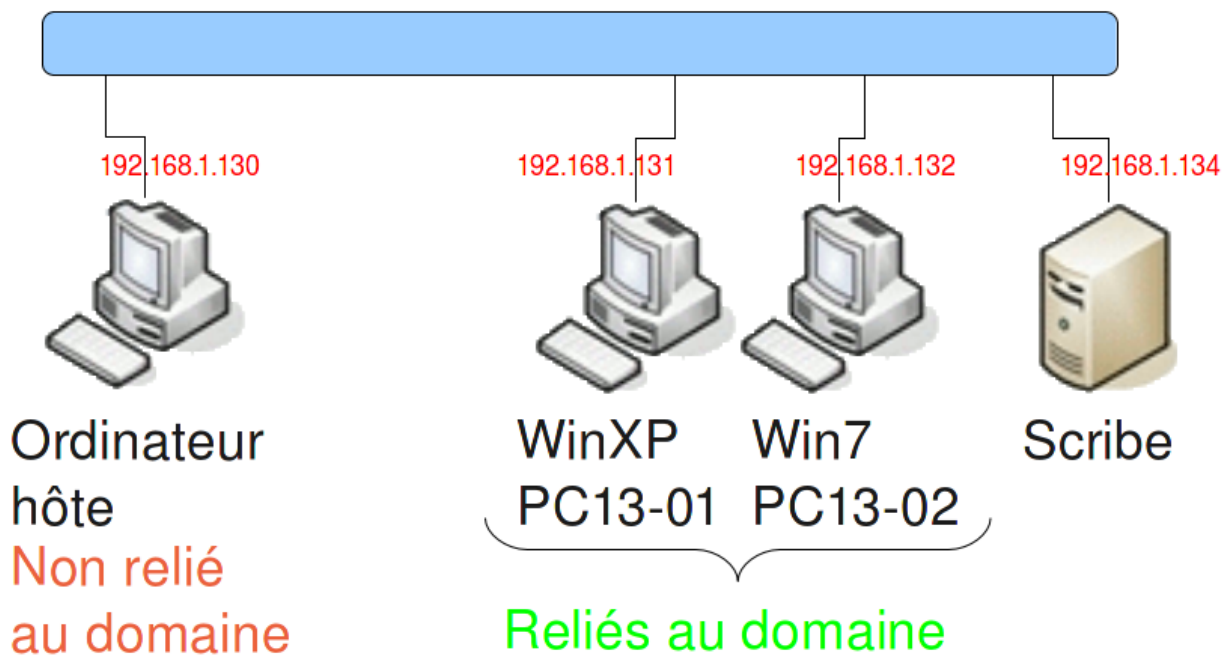


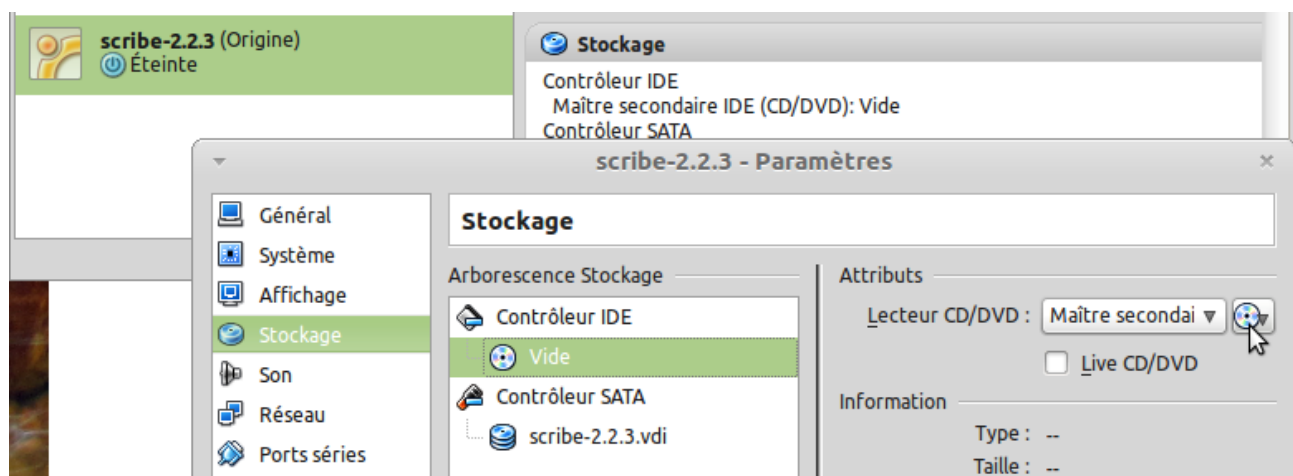
FIGURE 4 –

Notre travail maintenant est de créer la machine virtuelle qui va accueillir le système d'exploitation Linux sur lequel fonctionner.

Après avoir demandé la création d'une nouvelle machine dans VirtualBox, puis donné un nom (disons scribe) et choisi le type de système d'exploitation (ici Linux-Ubuntu), passez toutes les étapes en acceptant les choix par défaut (sauf pour la mémoire vive que nous passerons de 512Mo à 256Mo).

Une fois ces opérations terminées,

- cocher la case <> dans l'onglet «Processeur» de la section <> de votre machine virtuelle.
- choisir le mode d'accès par pont pour la carte réseau 1. Elle prendra ainsi une adresse sur le réseau sur lequel se trouve la machine hôte.
- L'image iso du dvd eole, téléchargée sur le site Eole <http://eoleng.ac-dijon.fr/pub/iso/> doit être montée comme un cd(ou dvd) virtuel, pour cela cliquez sur l'icône cd-rom dans l'onglet <>, comme sur l'image ci-dessous puis naviguez dans l'arborescence pour indiquer le fichier .iso.



On peut alors mettre en marche la machine virtuelle.

2 Mise en place du serveur

2.1 Installation



FIGURE 5 – image

Après avoir vérifié au niveau du BIOS que la machine démarre prioritairement sur le CD, le menu ci-contre apparaît.

Une bonne idée consiste à vérifier si le disque (le CD) a des défauts afin d'éviter de perdre du temps avec une installation qui échouerait sans doute.

Une fois ceci fait, lançons l'installation de Scribe. La procédure est automatique et vous n'avez qu'à observer les étapes

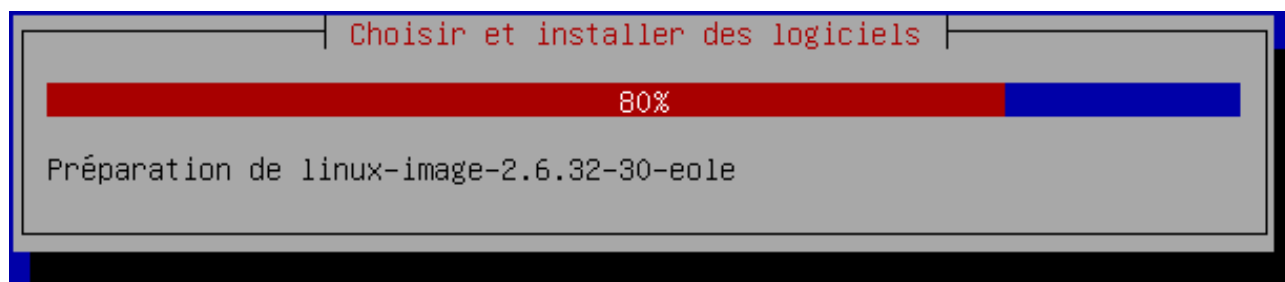


FIGURE 6 – image

Après redémarrage, le gestionnaire de démarrage GRUB vous propose plusieurs entrées. Nous choisissons celle par défaut

Vous pouvez maintenant vous identifier avec le login «root».

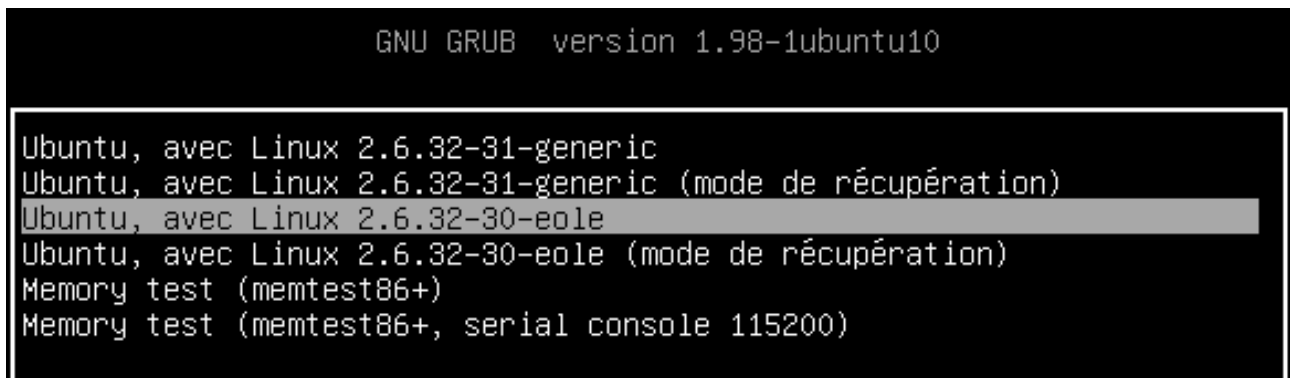


FIGURE 7 – image

- Pour scribe 2.2, le mot de passe est `eo!e`,
- Pour scribe 2.3, le mot de passe est `$eo!e&123456$`.

Avant de nous lancer dans la configuration de notre contrôleur de domaine scribe, notons ici quelques informations réseau dont nous aurons besoin pour configurer notre serveur :

- L’adresse IP fixe que nous allons lui attribuer :
- Le masque de sous-réseau :
- L’adresse de broadcast :
- L’adresse IP du ou des serveur(s) DNS :
 –
 –
- Le nom que nous donnerons à la machine :
- Le nom du domaine auquel les clients vont s’authentifier :
- Le mot de passe root : `dog!cat$mouse`
- Le mot de passe eole ou scribe : `fox!bird$fly`
- Le mot de passe admin : `plop`

root : utilisateur linux ; a tous les droits sur le serveur

scribe : utilisateur linux ; peut faire certains tests via une interface graphique

admin : utilisateur samba ; gestionnaire des machines une fois celles-ci connectées au domaine , c’est l’administrateur réseau).

Mise à jour :

```
root@scribeng:~#Maj-Auto -i
```

Saisissez la commande `gen_config` qui va lancer le générateur de configuration

```
root@scribeng:~#gen_config
```

La série d’écrans est à renseigner en étant très attentif.

2.1.1 Configuration scribe 2.2

Voir figures 8 à 11.

2.1.2 Configuration scribe 2.3

Voir figures ?? à ??.

2.1.3 Instanciation

General	Adresse IP de la carte eth0	192.168.0.105	Prec	Def
Services	Masque de sous réseau de la carte eth0	255.255.255.0	Prec	Def
Service-sso	Adresse réseau de la carte eth0	192.168.0.0	Prec	Def
Envole	Adresse de broadcast de la carte eth0	192.168.0.255	Prec	Def
	Adresse IP de la passerelle par défaut	192.168.0.1	Prec	Def
	Adresse IP du DNS primaire	192.168.0.1	- +	Prec Def
	Autoriser les connexions SSH sur cette interface	non		Prec Def
	Utilisation d'un proxy	non		Prec Def
	Nom de la machine	scribe	Prec	Def
	Nom de domaine privé du réseau local	monreseau.lan	Prec	Def
	Nom de l'académie (ex : ac-dijon)	ac-paris.fr	Prec	Def
	Numéro RNE de l'établissement	0753344A	Prec	Def
	Nom de l'établissement	Lycée des oiseaux	Prec	Def
	Serveur de mise à jour	eoleng.ac-dijon.fr	Prec	Def
	Second serveur de mise à jour	ftp.crihan.fr	Prec	Def
	Niveau de mise à jour	minimum		Prec Def
	Gestion des logs centralisés	non		Prec Def
	Adresse serveur NTP	pool.ntp.org	- +	Prec Def

FIGURE 8 – Scribe 2.2

General	Nom du serveur de fichier (ex: monserveur)	scribe	Prec	Def
Services	Nom du domaine samba (ex: mondomaine)	oiseaux	Prec	Def
Service-sso	Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)	oiseaux.ac-paris.fr	Prec	Def
Envole	Nom DNS de la passerelle SMTP	smtp.nerim.fr	Prec	Def
	Activation de Cups	oui		Prec Def
	Activation du DHCP	non		Prec Def
	Activation de l'accès FTP	oui		Prec Def
	Activation du frontend Ead2	oui		Prec Def
	Applications web			
	Activation de l'accès à Eva-Web	oui		Prec Def
	Activation de l'accès à Gibii (b2i)	non		Prec Def
	Authentification SSO			
	Gestion du service SSO EOLE	oui		Prec Def
	Utilisation du service sso pour les applications de votre serveur scribe	non		Prec Def

FIGURE 9 – Scribe 2.2

General	Configuration du serveur SSO			
Services	Adresse IP du serveur d'authentification	192.168.0.105	Prec	Def
Service-ss0	Port utilisé par le service SSO	8443	Prec	Def
Envole	Adresse du serveur ldap utilisé par le SSO	localhost	-	+
	Port du serveur ldap utilisé par le SSO	389	Prec	Def
	Chemin de recherche dans l'annuaire	o=gouv,c=fr	Prec	Def
	Version du protocole CAS émulé	2	Prec	Def
	Adresse du serveur SSO parent		Prec	Def
	Port du serveur SSO parent	8443	Prec	Def
	Chemin du certificat SSL (ou rien)		Prec	Def
	Chemin de l'autorité de certification (ou rien)		Prec	Def
	Durée en secondes de vie d'une session sur le serveur SSO	7200	Prec	Def
	CSS par défaut du service SSO (sans le .css)		Prec	Def
	Cacher le formulaire lors de l'envoi des informations de fédération	non	Prec	Def
	Configuration de l'authentification CAS			

FIGURE 10 – Scribe 2.2

General	EnvOLE 1.5			
Services	Activer l'accès à EnvOLE 1.5	non	Prec	Def
Service-ss0	EnvOLE 2			
Envole	Activer l'accès à EnvOLE 2	non	Prec	Def
	Configuration Commune			
	Activation de l'accès à Webshare (gestionnaire de fichiers)	oui	Prec	Def
	Activation de l'accès au cahier de texte Chocolat	non	Prec	Def
	Activation de l'accès à Grr (gestion des ressources)	non	Prec	Def
	Activation du gestionnaire de tâche Taskfreak	non	Prec	Def
	Activation de l'accès à Webcalendar	non	Prec	Def
	Activation de l'accès à Wordpress (blog)	non	Prec	Def

FIGURE 11 – Scribe 2.2

<ul style="list-style-type: none"> General Services Messagerie Interface-0 Clamav Bacula Esu Eole-ssso Applications web 	Etablissement		
	Identifiant de l'établissement (exemple UAI)	0753344A	Prec De
	Nom de l'établissement	Lycée des oiseaux	Prec De
	Paramètres réseau globaux		
	Nom de la machine	scribe	Prec De
	Nom de domaine privé du reseau local	monreseau.lan	Prec De
	Nom de domaine académique (ex : ac-dijon)	ac-paris.fr	Prec De
	Suffixe du nom de domaine académique (ex : fr)	fr	Prec De
	Utiliser un proxy	non	Prec De
	Valeur 1 ✕ +		
	Adresse serveur NTP	pool.ntp.org	Prec De
	Valeur 1 ✕ +		
	Adresse IP du serveur DNS	192.168.0.1	Prec De
	Mise à jour		
	Niveau de mise à jour	minimum	Prec De
Valeur 1 ✕ Valeur 2 ✕ +			
Serveur de mise à jour	eoleng.ac-dijon.fr	Prec De	
Fuseau horaire du serveur	Europe/Paris	Prec De	
Domaine Samba			
Nom du serveur de fichier (ex: monserveur)	scribe	Prec De	
Nom du domaine Samba (ex: mondomaine)	oiseaux	Prec De	
<div> <div>Valider groupe</div> <div>Charger default pour groupe</div> </div>			

FIGURE 12 – Scribe 2.3

<ul style="list-style-type: none"> General Services Messagerie Interface-0 Clamav Bacula Esu Eole-ssso Applications web 	Activer la gestion de l'onduleur NUT	non	Prec Def
	Activer l'anti-virus ClamAV	oui	Prec Def
	Activer la sauvegarde Bacula	oui	Prec Def
	Activer DHCP	non	Prec Def
	Activer l'accès FTP	oui	Prec Def
	Activer le serveur d'impression CUPS	oui	Prec Def
	Utiliser un serveur EOLE-SSO	local	Prec Def
	Activer le serveur web Apache	oui	Prec Def
	<div> <div>Valider groupe</div> <div>Charger default pour groupe</div> </div>		

FIGURE 13 – Scribe 2.3

General	Passerelle SMTP		smtp.nerim.fr	Prec	Def
Services	Utilisation du TLS (SSL) par la passerelle SMTP	non	Prec	Def	
Messagerie	Adresse mail d'envoi pour le compte root		Prec	Def	
Interface-0	Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)	oiseaux.ac-paris.fr	Prec	Def	
Clamav	Taille des boîtes aux lettres en Mo	20	Prec	Def	
Bacula	Activer le serveur de listes de diffusion Sympa	oui	Prec	Def	
Esu	Activer le service anti-spam SpamAssassin	oui	Prec	Def	
Eole-sso	Activer le serveur de courrier	imap	Prec	Def	
Applications web					
Valider groupe		Charger default pour groupe			

FIGURE 14 – Scribe 2.3

General	Configuration de l'interface				
Services	Méthode d'attribution de l'adressage pour l'interface	statique	Prec	Def	
Messagerie	Adresse IP de la carte	192.168.0.105	Prec	Def	
Interface-0	Masque de sous réseau de la carte	255.255.255.0	Prec	Def	
Clamav	Adresse réseau de la carte	192.168.0.0	Prec	Def	
Bacula	Adresse broadcast de sous réseau de la carte	192.168.0.255	Prec	Def	
Esu	Adresse IP de la passerelle par défaut	192.168.0.1	Prec	Def	
Eole-sso	Administration distante sur l'interface				
Applications web	Autoriser les connexions ssh	non	Prec	Def	
Bacula	Autoriser les connexions pour administrer le serveur (EAD, Sympa, ...)	oui	Prec	Def	
Esu	Valeur 1 ✕ +				
Eole-sso	Adresse IP réseau autorisé	192.168.0.0	Prec	Def	
Applications web	Masque du sous réseau	255.255.255.0	Prec	Def	
Configuration des alias sur l'interface					
	Ajouter des IP alias sur l'interface	non	Prec	Def	
Configuration des VLAN sur l'interface					
	Activer le support des VLAN sur l'interface	non	Prec	Def	
Valider groupe		Charger default pour groupe			

FIGURE 15 – Scribe 2.3

General	Activer l'anti-virus temps réel sur SMB	oui	Prec	Def
Services	Activer l'anti-virus temps réel sur FTP	oui	Prec	Def
Messagerie	Durée de conservation des fichiers en quarantaine (en jours)	20	Prec	Def
Interface-0	Activer l'antivirus sur la messagerie	oui	Prec	Def
Clamav				
Valider groupe		Charger default pour groupe		

FIGURE 16 – Scribe 2.3

General	Configuration du directeur			
Services	Activer le directeur localement	oui	Prec	Def
Messagerie	Nom du directeur local	scribe-dir	Prec	Def
Interface-0	Période de rétention des sauvegarde complètes	6	Prec	Def
Clamav	Unité de valeur pour la rétention des sauvegardes complètes	months	Prec	Def
Bacula	Période de rétention des sauvegarde différentielles	5	Prec	Def
Esu	Unité de valeur pour la rétention des sauvegardes différentielles	weeks	Prec	Def
Eole-ss0	Période de rétention des sauvegarde incrémentales	10	Prec	Def
Applications web	Unité de valeur pour la rétention des sauvegardes incrémentales	days	Prec	Def
Configuration du stockage				
	Activer le serveur de stockage localement	oui	Prec	Def
Autoriser des directeurs à se connecter au stockage				
	Valeur 1 ✕	+		
Valider groupe		Charger default pour groupe		

FIGURE 17 – Scribe 2.3

Esu	Activer le proxy ESU	non	Prec	Def
-----	----------------------	-----	------	-----

FIGURE 18 – Scribe 2.3

General	Nom de domaine du serveur d'authentification SSO		192.168.0.105	Prec
Services	Port utilisé par le service EOLE-SSO		8443	Prec
Messagerie	Valeur 1 ✕ +			
Interface-0	Adresse du serveur LDAP utilisé par EOLE-SSO		localhost	Prec
Clamav	Port du serveur LDAP utilisé par EOLE-SSO		389	Prec
Bacula	Chemin de recherche dans l'annuaire		o=gouv,c=fr	Prec
Esu	Libellé à présenter aux utilisateurs en cas d'homonymes		Annuaire de scribe.monreseau.lk	Prec
Eole-sso	Utilisateur de lecture des comptes LDAP (nécessaire pour la fédération)		cn=reader,o=gouv,c=fr	Prec
Applications web	Fichier de mot de passe de l'utilisateur de lecture		/root/.reader	Prec
		Adresse du serveur SSO parent		Prec
		Port du serveur SSO parent	8443	Prec
		Chemin du certificat SSL (ou rien)		Prec
		Chemin de l'autorité de certification (ou rien)		Prec
		<div> <div>Valider groupe</div> <div>Charger défaut pour groupe</div> </div>		

FIGURE 19 – Scribe 2.3

General	URL d'accès aux applications web (sans http://)		192.168.0.105	Prec	Def
Services	Application web par défaut (redirection)		/webmail	Prec	Def
Messagerie	Activer SquirrelMail (webmail)		oui	Prec	Def
Interface-0	Activer phpMyAdmin		non	Prec	Def
Clamav	Activer Ajaxplorer (gestionnaire de fichiers)		oui	Prec	Def
Bacula					
Esu					
Eole-sso					
Applications web					
		<div> <div>Valider groupe</div> <div>Charger défaut pour groupe</div> </div>			

FIGURE 20 – Scribe 2.3