Mise en service HIN Access Gateway (liste de contrôle)

Cette liste de contrôle énumère toutes les activités qui doivent être effectuées pour une mise en service réussie du HIN Access Gateway.

[ ] Conditions préalables à l'intégration du HIN Access Gateway

Pour que l'AGW puisse effectuer le Single Sign-on, il vérifie l'utilisateur avec l'Active Directory. L'AGW peut communiquer avec l'Active Directory de la manière suivante:

- LDAP TLS ou LDAPS
- NTLM ou Kerberos

Conditions préalables à prendre en compte:

- Public IP fixe ou plage Public IP fixe du client et de l'AGW
- URL interne avec résolution DNS sur le nom d'hôte AGW
- Serveur AD (on Prem ; à partir de 2016) (actuellement, un seul domaine est supporté)
- Serveur AD avec certificat SSL (manuel AGW, chapitre 5.1)
- Certificat SSL pour AGW (d'une CA connue du navigateur) (manuel AGW, chapitre 4.5)
- Ports de pare-feu selon liste (manuel AGW, chapitre 3.3.2)
- Si Kerberos est utilisé; utilisateur LDAP en lecture seule (manuel AGW, chapitre 5.2.cf)
- Adresse e-mail pour les notifications (avis de mise à jour) (manuel AGW, chapitre 4.4.7)
- Configuration du navigateur client par GPO (manuel AGW, chapitre 6)

[ ] Dimensionnement de la HIN Access Gateway Appliance

Dimensionnement		Les ressources suivantes sont nécessaires pour une Virtual Appliance:
[ ]	**Mémoire**	2 Go
[ ]	**Espace disque**	5 Go
[ ]	**CPU**	1 CPU virtuelle

[ ] Utilisation du HIN Access Gateway en tant que Virtual Appliance

Type		**Caractéristiques**	**Avantages**
[ ]	**Virtual Appliance**	Virtual Appliance basée sur Linux, utilisable sous VMWare ESX et Microsoft Hyper-V	Utilisation de l'infrastructure virtualisée existante (ressources, redondances, surveillance, etc.)

[ ]	**Entrée DNS**		
	Pour la connexion via le HIN Access Gateway, une entrée DNS interne est nécessaire, laquelle est également indiquée lors de l'enregistrement sur HIN (Auth URL). – Celle-ci doit pouvoir être résolue par les clients se trouvant sur votre LAN. Si vous utilisez Kerberos, nous vous recommandons de donner le même nom au nom d'hôte AGW et à l'entrée DNS.		
	AGW VM	**DNS Record**	**Valeur**

Si vous avez un nom de domaine interne avec .local, veuillez lire attentivement le point du manuel.

Sont supportés:

- 1 AD (avec les méthodes suivantes: LDAP / LDAPS, NTLM ou Kerberos)
- Mapping des groupes OU/AD sur certains AGW ID ou Team ID; veuillez consulter le manuel à ce sujet.
- Les utilisateurs peuvent associer l'eID HIN à leur compte AD personnel. (Les utilisateurs existants qui utilisent le client HIN doivent avoir activé l'accès SMS («code SMS») dans le Servicecenter.)

[ ]	**Activation de ports dans le pare-feu ou le routeur**			
	Port	**Source**	**Objectif**	**Description**
[ ]	TCP 443 (https)	HIN Access Gateway(s)	gateway2.hin.ch app.hin.ch auth.hin.ch agw-manager.hin.ch	Connexion au centre de données HIN pour l'accès aux applications.
[ ]	TCP 443 (https)	Clients (utilisateurs finaux)	HIN Access Gateway(s)	Accès à l'Access Gateway pour l'authentification
[ ]	TCP 389 (ldap)	HIN Access Gateway(s)	HIN Access Gateway(s)	Vérification du login de l'AD
[ ]	TCP 636 (ldaps)	HIN Access Gateway(s)	Active Directory	Vérification du login de l'AD
[ ]	**TCP 88 (Kerberos)**	HIN Access Gateway(s)	Active Directory	Vérification du token Kerberos
[ ]	TCP 2222 (ssh)	HIN Access Gateway(s)	update2.agw.hin.ch	Connexion au centre de données HIN pour la connexion de support
[ ]	TCP 80 (http)	HIN Access Gateway(s)	update2.agw.hin.ch	Obtention de mises à jour du système
[ ]	TCP 4433	Admin-clients	HIN Access Gateway(s)	HIN AGW Adminport
	Cluster: Activation de ports si l'AGW est exploité dans un cluster			
[ ]	TCP 22 (ssh)	Entre tous les nœuds de cluster		Nécessaire pour la synchronisation des paramètres du cluster
[ ]	UDP 5404 - 5406	Entre tous les nœuds de cluster		Requis pour changer l'adresse IP virtuelle

[ ]	**Paramètres réseau HIN Access Gateway**		
	[ ]	**Adresse IP interne HIN Access Gateway Appliance**	
	[ ]	**Masque de réseau**	
	[ ]	**Nom d'hôte HIN Access Gateway**	
	[ ]	**Adresse IP Default / Standard Gateway**	
	[ ]	**Adresse IP serveur DNS 1**	
	[ ]	**Adresse IP serveur DNS 2**	
	[ ]	**DC 1 et DC 2**	
	[ ]	**Plage(s) d'adresses IP externes dans laquelle/lesquelles se trouvent les clients et la HIN Access Gateway Virtual Appliance (visible sur HIN)**	

[ ]	**Configuration en cluster**		
	Le clustering permet d'accroître la disponibilité du HIN Access Gateway.		
	[ ]	**Aucun cluster**	
	[ ]	**Cluster**	
		Adresses IP physiques	
		[ ] **Adresse IP interne du second HIN Access Gateway**	
		[ ] **Adresse IP externe du second HIN Access Gateway**	
		Adresses IP virtuelles	
		[ ] **Adresse IP virtuelle commune aux deux instances HIN Access Gateway** Le nom de l'entrée AGW DNS est le même que l'IP virtuelle.	

[ ]	**Coordination avec HIN**	
	[ ]	**Fixation de la date de mise en service avec le support HIN** La mise en service comprend une phase de test d'une heure. Pendant ce laps de temps, l'Access Gateway est enregistré et l'accès au répertoire des participants HIN est testé afin de vérifier la réussite de la mise en service du HIN Access Gateway. Pour cela, un rendez-vous doit être pris avec le gestionnaire d'intégration HIN.

[ ]	**Clarification des tâches d'exploitation**		
	[ ]	**Clarification des tâches d'exploitation et des responsabilités**	
	[ ]	**Exploitation technique**	
		[ ] **Planification des sauvegardes périodiques**	
		[ ] **Planification de la mise en place de la surveillance / intégration dans l'infrastructure de surveillance**	
		[ ] **Organisation du contrôle régulier des fichiers journaux**	
		[ ] **Organisation des mises à jour régulières (notification par e-mail)**	
	[ ]	**Organisation du support pour les utilisateurs internes (technique / professionnel)**	