HIN Access Gateway Inbetriebsetzung (Checkliste)

In dieser Checkliste sind alle Tätigkeiten aufgeführt, die für eine erfolgreiche Inbetriebsetzung des HIN Access Gateways durchgeführt werden müssen.

[ ] Voraussetzungen für die Integration des HIN Access Gateway

Damit der AGW das Single Sign-on durchführen kann, überprüft er den Benutzer mit dem Active Directory. Der AGW kann mit dem Active Directory wie folgt kommunizieren:

- LDAP TLS oder LDAPS
- NTLM oder Kerberos

Zu berücksichtigende Voraussetzungen:

- Fixe Public IP oder fixe Public IP Range von Client und AGW
- Interne URL mit DNS-Auflösung auf Hostname AGW
- AD Server (on Prem; ab 2016) (zurzeit wird nur eine Domain unterstützt)
- AD Server mit SSL-Zertifikat (Handbuch AGW, Kapitel 5.1)
- SSL-Zertifikat für AGW (von einer CA die dem Browser bekannt ist) (Handbuch AGW, Kapitel 4.5)
- Firewall Ports gemäss Liste (Handbuch AGW, Kapitel 3.3.2)
- Falls Kerberos verwendet wird; LDAP read-only Benutzer (Handbuch AGW, Kapitel 5.2 ff)
- E-Mail-Adresse für Notifications (Update-Avisierung) (Handbuch AGW, Kapitel 4.4.7)
- Konfiguration der Client Browser per GPO (Handbuch AGW, Kapitel 6)

[ ] Dimensionierung der HIN Access Gateway Appliance

Dimensionierung		Folgende Ressourcen werden für eine Virtual Appliance benötigt:
[ ]	**Memory**	2 GB
[ ]	**Diskplatz**	5 GB
[ ]	**CPU**	1 virtuelle CPUs

[ ] Einsatz des HIN Access Gateways als Virtual Appliance

Typ		Merkmale	Vorteile
[ ]	**Virtual Appliance**	Virtual Appliance auf Basis Linux, einsetzbar unter VMWare ESX und Microsoft Hyper-V	Nutzung der vorhandenen virtualisierten Infrastruktur (Ressourcen, Redundanzen, Monitoring, usw.)

[ ]	**DNS Eintrag**		
	Für die Anmeldung über den HIN Access Gateway wird ein interner DNS-Eintrag benötigt, welcher auch bei der Registration bei HIN angegeben wird (Auth URL). – Dieser muss von den sich in Ihrem LAN befindenden Clients aufgelöst werden können. Falls Sie Kerberos benutzen, empfehlen wir Ihnen, dass der AGW Hostname und der DNS-Eintrag gleich lauten.		
	AGW VM	**DNS Record**	**Wert**

Wenn Sie einen internen Domainnamen mit .local haben, lesen Sie bitte Punkt im Handbuch sorgfältig durch.

Unterstützt:

- 1 AD (mit folgenden Methoden: LDAP / LDAPS, NTLM oder Kerberos)
- Mapping OU/AD Groups auf bestimmte AGW ID oder Team IDs, bitte konsultieren Sie hierfür das Handbuch.
- Benutzer können die HIN eID mit Ihrem persönlichen AD-Konto verknüpfen. (Bestehende Benutzer, die den HIN Client verwenden, müssen im Servicecenter den SMS-Zugang («SMS Code») aktiviert haben.)

[ ]	**Freischaltung von Ports in der Firewall bzw. im Router**				
		Port	**Quelle**	**Ziel**	**Beschreibung**
	[ ]	TCP 443 (https)	HIN Access Gateway(s)	gateway2.hin.ch app.hin.ch auth.hin.ch agw-manager.hin.ch	Verbindung zu HIN RZ für Applikationszugriff.
	[ ]	TCP 443 (https)	Clients (Endanwender)	HIN Access Gateway(s)	Zugriff auf Access Gateway zur Authentisierung
	[ ]	TCP 389 (ldap)	HIN Access Gateway(s)	HIN Access Gateway(s)	Verifizierung des AD-Logins
	[ ]	TCP 636 (ldaps)	HIN Access Gateway(s)	Active Directory	Verifizierung des AD-Logins
	[ ]	**TCP 88 (Kerberos)**	HIN Access Gateway(s)	Active Directory	Verifizierung des Kerberos Tokens
	[ ]	TCP 2222 (ssh)	HIN Access Gateway(s)	update2.agw.hin.ch	Verbindung zum HIN RZ für die Support-Connection
	[ ]	TCP 80 (http)	HIN Access Gateway(s)	update2.agw.hin.ch	Bezug von System Updates
	[ ]	TCP 4433	Admincli-ents	HIN Access Gateway(s)	HIN AGW Adminport
	Cluster: Freischaltung von Ports wenn der AGW im Cluster betrieben wird				
	[ ]	TCP 22 (ssh)	Zwischen allen Cluster Nodes		Benötigt für die Synchronisation der Cluster-Einstellungen
	[ ]	UDP 5404 - 5406	Zwischen allen Cluster Nodes		Benötigt für das Wechseln der virtuellen IP-Adresse

[ ]	**Netzwerkparameter HIN Access Gateway**		
	[ ]	**Interne IP-Adresse HIN Access Gateway Appliance**	
	[ ]	**Netzmaske**	
	[ ]	**Hostname HIN Access Gateway**	
	[ ]	**IP-Adresse Default / Standard Gateway**	
	[ ]	**IP-Adresse DNS Server 1**	
	[ ]	**IP-Adresse DNS Server 2**	
	[ ]	**DC 1 und DC 2**	
	[ ]	**Externe IP-Adresse Range(s) in welcher sich die Cients und die HIN Access Gateway Appliance (bei HIN sichtbar)**	

[ ]	**Clusterkonfiguration**		
	Durch Clustering kann die Verfügbarkeit des HIN Access Gateways erhöht werden.		
	[ ]	**Kein Cluster**	
	[ ]	**Cluster**	
		Physische IP-Adressen	
		[ ] **Interne IP-Adresse des zweiten HIN Access Gateways**	
		[ ] **Externe IP-Adresse des zweiten HIN Access Gateways**	
		Virtuelle IP-Adressen	
		[ ] **Gemeinsame virtuelle IP-Adresse beider HIN Access Gateway Instanzen** Der AGW DNS-Eintrag lautet auf die virtuelle IP.	

[ ]	**Koordination mit HIN**	
	[ ]	**Vereinbarung des Produktivschaltungstermins mit dem HIN Support** Die Produktivschaltung beinhaltet eine Testphase von einer Stunde. In dieser Zeit wird der Access Gateway registriert und der Zugriff auf das HIN Teilnehmerverzeichnis getestet, um die erfolgreiche Inbetriebsetzung des HIN Access Gateways zu prüfen. Dafür muss ein Termin mit dem HIN Integration Manager vereinbart werden.

[ ]	**Klärung der Betriebsaufgaben**		
	[ ]	**Klären der betrieblichen Aufgaben und Verantwortlichkeiten**	
	[ ]	**Technischer Betrieb**	
		[ ] **Planung des periodischen Backups**	
		[ ] **Planung Aufsetzen des Monitorings / Einbindung in die Monitoring-Infrastruktur**	
		[ ] **Organisation der regelmässigen Prüfung der Logfiles**	
		[ ] **Organisation der regelmässigen Updates (Notification Mail)**	
	[ ]	**Support für interne Benutzer organisieren (technisch / fachlich)**	