

HPE Aruba Networking EdgeConnect Cloud Orchestrator

Příloha II: Popis způsobu zpracování

1.	Popis způsobu zpracování	<p>HPE Aruba Networking EdgeConnect Cloud Orchestrator poskytuje moderní, cloudově orientovaný provoz sítě a zajištění pro sítě SD-WAN a integraci řešení Security Service Edge (SSE).</p> <p>HPE Aruba Networking EdgeConnect Cloud Orchestrator poskytuje centralizovanou správu a organizaci rozbočovačů a bran SD-WAN, včetně uspořádání překrývajících se podnikových sítí (překrývajících se virtuálních sítí), zásad firewallu a zásad optimalizace aplikací.</p> <p>Vedle toho HPE Aruba Networking EdgeConnect Cloud Orchestrator umožňuje shromažďovat určitá data související s využíváním funkcí pro optimalizaci produktů při nasazení v prostředích SD-WAN.</p>
2a.	Druhy zpracovávaných osobních údajů, Základní scénář se standardními funkcemi:	<p>Osobní údaje shromážděné v rámci správy sítě a souvisejících aplikací zahrnují:</p> <ul style="list-style-type: none">— IP adresa koncového uživatele— E-mailová adresa a kontaktní údaje uživatele s rolí správce— Připojení uživatelů k aplikacím a webovým doménám (bez protokolování)
2b.	Typ dodatečně zpracovávaných osobních údajů, — Scénář s integrací VXLAN:	<ul style="list-style-type: none">— Role uživatele
2c.	Typ dodatečně zpracovávaných osobních údajů, — Scénář s Radius Snooping nebo — Integrace rovin správy s poskytovatelem identity	<ul style="list-style-type: none">— Role uživatele— Uživatelské jméno— Zařízení uživatele— MAC adresa uživatele— Uživatelská skupina— Uživatelská síť VLAN

Příloha II: Popis způsobu zpracování (pokračování)

3.	Kategorie zpracovávaných osobních údajů	Správci koncoví uživatelé, zaměstnanci, dodavatelé a dočasní pracovníci
4.	Doba zpracování	Informace shromažďované a ukládané řešením jsou minimem potřebným k podpoře zajištění bezpečného přístupu k portálu a jsou nezbytné pro plnění jeho funkce. Všechny protokoly relací o uživateli s rolí správce se automaticky vymažou po 365 dnech.
5.	Technická a organizační opatření	Zpracovatel dodržuje program informační a fyzické bezpečnosti pro ochranu osobních údajů správce, jak je podrobně uvedeno v příloze III níže

Příloha III: Technická a organizační opatření včetně technických a organizačních opatření na podporu zajištění bezpečnosti údajů

— Bezpečnostní funkce produktu:

- **Fyzické zabezpečení:** Služba HPE Aruba Networking EdgeConnect Cloud Orchestrator je hostována na nejrozšířenější platformě IaaS – Amazon Web Services (AWS) – která nabízí nejkomplexnější funkce zabezpečení a dodržování předpisů. AWS zavedla bezpečnostní opatření ve všech kritických oblastech včetně perimetru, infrastruktury, dat a prostředí.
- **Zabezpečení sítě:** Zabezpečení sítě zpracovatele pomáhá zajišťovat bezpečnost fyzické a virtuální sítě, v níž se aplikace a data nacházejí. Využíváme služby a nástroje, které nabízí poskytovatel IaaS, a některá řešení třetích stran, abychom zajistili maximální zabezpečení našeho produkčního prostředí před vnějšími hrozbami a vnitřními zranitelnostmi. Zpracovatel provozuje oddělené instance interních a produkčních prostředí. Interní prostředí je zaměřeno na vývoj a testování, zatímco produkční prostředí je vyhrazeno výhradně pro naše zákazníky (správce). Toto fyzické a logické oddělení našeho produkčního prostředí od ostatních běžících instancí zpracovateli pomáhá nabízet co nejkvalitnější nasazení softwaru pro naše zákazníky (správce) a pomáhá zajistit, aby jejich data byla vždy omezena na jedno prostředí.
- **Architektura a zabezpečení aplikace:** Veškerý provoz, který se vyměňuje mezi aplikací a okolním světem, probíhá pomocí protokolu HTTPS přes TLS. HPE Aruba Networking EdgeConnect Cloud Orchestrator nabízí izolaci klientů.
- **Zabezpečení dat:** Veškerá výměna dat mezi aplikací, zařízeními a uživateli probíhá pomocí protokolu HTTPS. Data v klidovém stavu jsou šifrována a ukládána. Data jsou pravidelně zálohována a záložní data jsou ukládána redundantně. Z organizačního hlediska máme k dispozici tým DevOps, který spravuje všechny bezpečnostní a provozní aspekty aplikace.
- **Geografická dostupnost:** Služba HPE Aruba Networking EdgeConnect Cloud Orchestrator je dostupná na několika místech po celém světě, takže si správce může vybrat, ve kterém regionu si založí účet. Toto rozhodnutí může záviset na mnoha faktorech. Organizace může například vyžadovat, aby byla všechna data uložena v určitém regionu, nebo může stanovit regulační omezení týkající se způsobu zpracování a ukládání dat.

Služba HPE Aruba Networking EdgeConnect Cloud Orchestrator je nasazena v clusterech ve vybraných datových centrech Amazon Web Services (AWS), přičemž AWS dodává infrastrukturu potřebnou k ukládání a zpracování dat. V následující tabulce najdete podrobný seznam clusterů a oblastí podpory řešení AWS pro HPE Aruba Networking EdgeConnect Cloud Orchestrator:

US-2	Východní část USA (Severní Virginie)
Východní část USA 2	Východní část USA (Ohio)
Evropská unie 1	EU (Frankfurt)
Jižní část Asie a Tichomoří 1	Asie a Tichomoří (Bombaj)
Jihovýchodní část Asie a Tichomoří	Asie a Tichomoří (Sydney)

Veškerá správa a organizace poskytovaná službou HPE Aruba Networking EdgeConnect Cloud Orchestrator na zařízeních nebo branách SD-WAN je spojena s vyhrazenými instancemi výpočetních operací a databázových úložišť určených pro konkrétní klienty.

Všechna data (včetně osobních údajů) pro služby HPE Aruba Networking EdgeConnect Cloud Orchestrator a veškerá další uživatelská data jsou ukládána v databázích v rámci stejné výpočetní instance.

Jakékoli další zpracování, které může být vyžadováno, probíhá rovněž na výpočetních instancích v rámci stejné výpočetní instance nebo jiným způsobem v souladu s podmínkami DPSA pro síťové produkty HPE Aruba Networking.

Bezpečnostní opatření:

- Zpracovatel dodržuje následující program informační a fyzické bezpečnosti pro ochranu osobních údajů správce (bezpečnostní program zpracovatele):
 - Infrastruktura zpracovatele má k dispozici aktualizované verze bezpečnostního softwaru systému, což může zahrnovat bránu firewall na bázi hostitele, antivirovou ochranu a nejnovější opravy chyb či definice nových virů. Zpracovatel uchovává protokoly o událostech týkajících se infrastruktury, včetně systémů detekce narušení, aby mohl sledovat, odhalovat a hlásit vzory zneužití, podezřelé činnosti, neoprávněné uživatele a další bezpečnostní rizika.
 - Zaměstnanci a smluvní partneři jsou proškoleni o zásadách ochrany osobních údajů a zabezpečení zpracovatele a jsou seznámeni se svými povinnostmi v oblasti ochrany osobních údajů a zabezpečení. Zaměstnanci a smluvní partneři zpracovatele jsou smluvně zavázáni zachovávat důvěrnost osobních údajů správce a dodržovat příslušné zásady, normy nebo požadavky zpracovatele v souvislosti se zpracováním osobních údajů správce. Nedodržení těchto zásad, standardů nebo požadavků bude předmětem vyšetřování, které může vyústit v disciplinární opatření až do ukončení pracovního poměru nebo angažmá u zpracovatele.
- Pokud se správce dozví o incidentu narušení bezpečnosti osobních údajů, který má vliv na služby, neprodleně o tom informuje zpracovatele a sdělí mu rozsah narušení bezpečnosti osobních údajů. Oznámení se odešle centru bezpečnostních operací zpracovatele e-mailem na adresu security@hpe.com.

Navštivte [HPE.com](https://www.hpe.com)

[Zahájit chat](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Informace obsažené v tomto dokumentu se mohou změnit bez předchozího upozornění. Jediné záruky na produkty a služby společnosti Hewlett Packard Enterprise jsou uvedeny v přesných vymezených prohlášeních týkajících se záruk, která jsou dodávána s těmito produkty a službami. Ze žádných zde uvedených informací nelze vyvodit existenci dalších záruk. Společnost Hewlett Packard Enterprise není zodpovědná za technické nebo redakční chyby ani za opomenutí vyskytující se v tomto dokumentu.

a50010933CSE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

