BEARCLAVE

Návrh architektury

Cílové prostředí Microsoft 365 a Azure

Verze	1.0
Zpracoval	Bearclave s.r.o.
Klasifikace	Veřejné — vzorový dokument

Bearclave s.r.o., Třešňová 916/16, Přímětice, 669 04 Znojmo
IČO 30007534 · DIČ CZ30007534 · zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 153837
info@bearclave.cz · bearclave.cz

1. Manažerské shrnutí

10	17	2	54 500 Kč
předplatných místo jednoho pokusného	pravidel prostředí, z toho 9 zakazujících	trvale privilegované účty, oba nouzové	orientačně měsíčně za ochranu a dohled

Organizace stěhuje provoz z vlastního datacentra do Azure. Dnes v cloudu stojí jen pokusné předplatné bez pravidel, kde tři lidé mají trvale roli Owner a dva servery mají RDP otevřené do internetu. Návrh místo něj staví sdílený základ pro identitu, dohled a síť a oddělená předplatná pro produkci a test každé ze tří aplikací.

Pravidla se nastaví jednou na management groups a každé nové předplatné je zdědí. Správce si roli aktivuje na hodiny a do produkce zapisuje jen pipeline po schválení druhou osobou. Zapnout ochranu a dohled naplno by stálo kolem 113 000 Kč měsíčně, aniž by organizace viděla víc.

Před realizací je potřeba rozhodnout osm otevřených bodů. Nejdůležitější je ochrana řadičů domény, na kterou licence Microsoft 365 E3 nestačí.

Návrh v kostce

Oblast	Návrh
Hierarchie	10 management groups ve 3 úrovních pod kořenem, 10 předplatných
Identity	12 rolí v modelu, privilegované jen jako oprávněné v PIM, 2 nouzové účty
Síť	hub-spoke s Azure Firewall, 7 spoků, VPN do centrály a dvou skladů
Baseline	17 pravidel, diagnostika, výstrahy, zámky, Defender for Cloud podle zátěže
Nasazení	Terraform a Terragrunt pro Azure, Microsoft365DSC pro Microsoft 365

2. Výchozí stav a požadavky

Organizace má přibližně 900 zaměstnanců, centrálu a dva sklady. Provoz běží na 46 virtuálních serverech VMware vSphere ve vlastním datacentru, jehož nájem končí za 14 měsíců. Návrh vznikl ze dvou workshopů, přístupu pro čtení k Azure a Entra ID a migračního plánu; aplikační architekturu, migraci ani obsazení rolí neřeší.

Oblast	Dnes
Identita	Active Directory s jednou doménou, Entra Connect Sync se synchronizací hash hesel
Licence	Microsoft 365 E3 pro všechny, Entra ID P2 pro 12 správců
Azure	pokusné předplatné bez hierarchie, politik a tagů; 3 přímá přiřazení Owner, 2 servery s RDP z internetu
Síť	sklady připojené do datacentra tunely IPsec z firewallů FortiGate
Stěhuje se	tři aplikace a řadiče domény; souborový server nahradí SharePoint, zbytek se vypne

Aplikace	Dnes	Cíl podle migračního plánu	Kdo přistupuje
Skladový systém	6 serverů Windows, SQL Server	virtuální servery, dodavatel nepodporuje PaaS	terminály skladů, kanceláře centrály
Zákaznický portál	4 servery Windows, IIS	App Service, Azure SQL Database	zákazníci z internetu
Integrační vrstva	3 servery: EDI, SFTP, API	API Management, Azure Functions, Service Bus	partneři z internetu, zápis do skladového systému

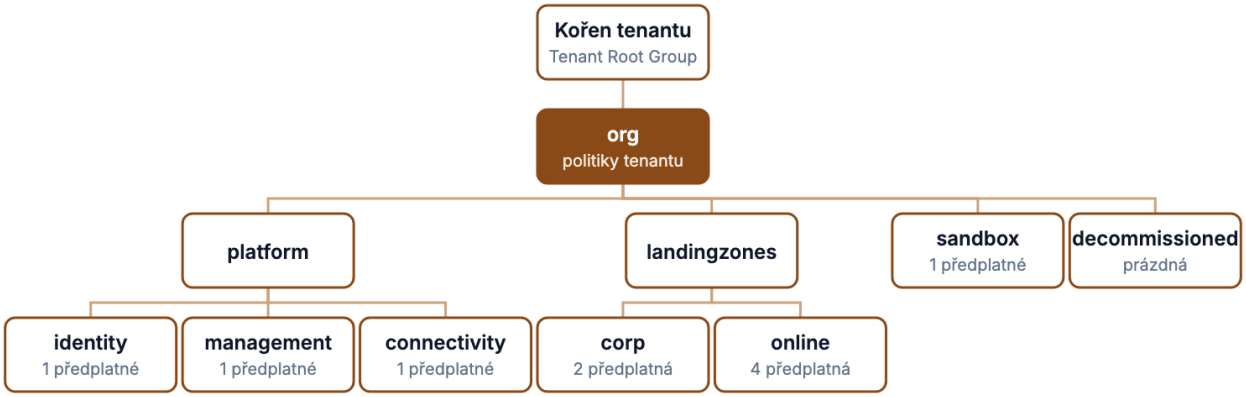
Požadavky organizace a jejich dopad na návrh

Požadavek	Dopad na návrh
Jeden region, obnova ze záloh	jeden hub, druhý region se zatím nestaví
Data zákazníků nesmí opustit EU	politika povolených regionů na kořeni org
Nákup přes Microsoft Customer Agreement	předplatná zakládá role na sekci faktury
Kód a pipeline v GitHub Enterprise Cloud	federace bez tajemství, schvalování nasazení
V neprodukci žádné produkční osobní údaje	oddělená předplatná, tag dataClassification
Microsoft Sentinel v příštím roce	jeden bezpečnostní pracovní prostor už teď
Microsoft 365 v kódu přes Microsoft365DSC	hranice mezi nástroji podle API
Hybridní identita zůstává	předplatné identity pro řadiče a Entra Connect
Řízení dopravníků nesmí záviset na cloudu	provozní síť skladů se do Azure nesměruje

3. Hierarchie a předplatná

Hierarchie vychází z referenční architektury Azure landing zones. Pravidla pro celý tenant nese mezilehlý kořen org, na Tenant Root Group se nic nepřiřazuje. Hloubka jsou tři úrovně pod kořenem, Azure jich dovoluje šest.

Management groups a počet předplatných



Předplatné	Skupina	Obsah a proč samostatně
sub-identity-prod	identity	řadiče domény, Entra Connect; správci identity
sub-management-prod	management	záznamy, stav a identity pipeline mimo provoz
sub-connectivity-prod	connectivity	hub, firewall, VPN, DNS, Bastion; jeden tým
sub-wms-prod, sub-wms-test	corp	skladový systém, bez vstupu z internetu
sub-portal-prod, sub-portal-test	online	zákaznický portál, vstup z internetu
sub-edi-prod, sub-edi-test	online	integrační vrstva, vstup partnerů
sub-sandbox-it	sandbox	pokusné předplatné bez spojení s firemní sítí

- Produkce a test sdílejí management group, takže co projde v testu, projde i v produkci. Rozdíl nesou předplatná: přístupy, plány ochrany a rozpočty.
- Corp a online se liší jen tím, zda aplikace přijímá provoz z internetu. Sandbox a decommissioned stojí mimo landingzones, aby nezdědily připojení k firemní síti.
- Nové předplatné zakládá role Azure subscription creator na sekci faktury. ID management group nejde po vytvoření změnit.
- Pokusné předplatné přejde do sandbox bez přímých přiřazení Owner. RDP se zavře ručně, politika stávající prostředky jen označí.

4. Identity a oprávnění

Model rolí určuje, kdo má na co dosah a v jakém režimu. Navrhuje role a skupiny, obsazení konkrétními lidmi je na organizaci.

Role v modelu	Oprávnění	Rozsah	Režim
Nouzový přístup	Global Administrator	tenant	trvale aktivní, 2 účty
Správa tenantu	Global Administrator, Privileged Role Administrator	tenant	oprávněná, schválení, 4 hodiny
Správa identit	User, Groups a Conditional Access Administrator	tenant	oprávněná, 8 hodin
Architekt platformy	Owner	org	oprávněná, schválení, 4 hodiny
Provoz platformy	Contributor	platform	oprávněná, schválení, 8 hodin
Provoz aplikace	Reader, Contributor	produkční předplatné aplikace	Reader aktivní, Contributor oprávněná se schválením
Vývoj aplikace	Contributor	testovací předplatné aplikace	aktivní
Bezpečnost	Security Reader, Security Admin	org	Reader aktivní, Admin oprávněná
Náklady	Cost Management Reader	org	aktivní
Pipeline, plán	Reader, čtení stavu, Directory Readers	org, tenant	identita úlohy, jen čtení
Pipeline, nasazení	Contributor, Resource Policy Contributor, vlastní role pro zámky, přidělování rolí s podmínkou, Directory Readers	org, tenant	identita úlohy, jen z prostředí prod
Pipeline, tenant	oprávnění aplikace v Microsoft Graph	tenant	identita úlohy, jen z prostředí prod

- Role se přiřazují jen skupinám a identitám úloh, nikdy přímo uživatelům. Noční kontrola hlásí každé přímé přiřazení.
- Privilegované role jsou oprávněné v PIM, role Azure přes oprávněné členství ve skupině. Aktivace vyžaduje MFA a odůvodnění, u produkce a práv navíc i schválení druhou osobou.

- Účet z Active Directory nedostane žádnou privilegovanou roli v cloudu, jinak by kompromitace domény znamenala i kompromitaci cloudu.
- Skupiny s rolemi Entra ID jsou přiřaditelné k rolím a jednou za čtvrtletí se nad nimi kontroluje přístup.

> Oprávněná přiřazení potřebují Entra ID P2 pro každého, kdo je má nebo schvaluje. Dnes je licencí 12, model počítá s dalšími přibližně deseti (otevřený bod 2).

4.1 Správci a nouzový přístup

- Každý správce má běžný účet z Active Directory a zvlášť správcovský účet jen v cloudu, bez pošty.
- Správcovský účet se přihlašuje jen odolnou metodou (FIDO2 nebo Windows Hello for Business) ze spravovaného zařízení. Vynucuje to Conditional Access se silou ověření.
- Server Entra Connect je na úrovni řadičů domény a spravují ho jen správci identity. Kdo ho ovládne, může měnit objekty v cloudu.
- Dva nouzové účty jen v cloudu na doméně onmicrosoft.com, každý se dvěma klíči FIDO2 v oddělených trezorech. Povinné MFA pro správu Azure platí i pro ně.
- Nouzové účty jsou vyjmuté ze všech politik Conditional Access statickou skupinou. Každé přihlášení spustí výstrahu, jednou za čtvrtletí se přihlášení zkouší.

4.2 Identity pipeline

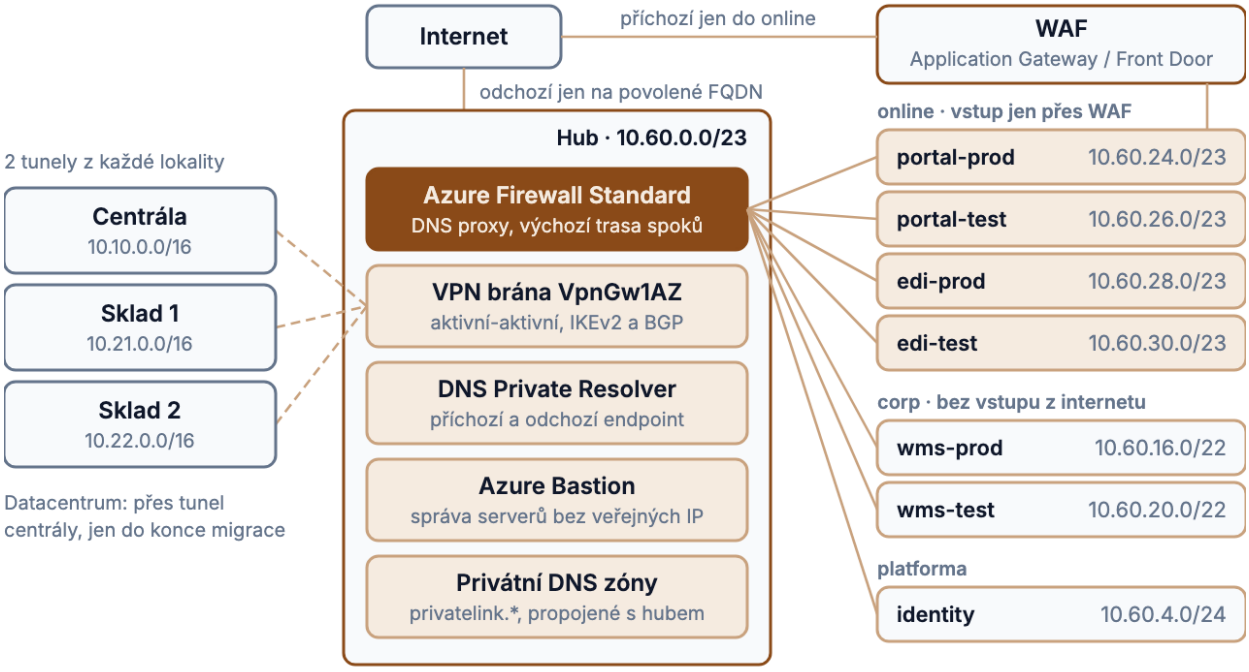
Pipeline se přihlašuje federací z GitHub Actions do spravovaných identit, takže žádné tajemství neexistuje.

- Plán je federovaný na pull request a na větev main pro noční drift. Workflow v pull requestu může upravit každý s právem zápisu do repozitáře, proto identita jen čte a plan běží bez zámku stavu.
- Nasazení je federované jen na prostředí prod, které přijímá větev main a čeká na schválení. Podmínka mu nedovolí přidělit Owner, User Access Administrator ani Role Based Access Control Administrator.
- Identita pipeline tenantu má v Graphu RoleManagement.ReadWrite.Directory, fakticky moc globálního správce. Repozitář je proto chráněný jako produkce.

5. Síť a bezpečnostní baseline

Návrh řeší síť v Azure a její propojení s centrálou, oběma sklady a po dobu migrace s datacentrem. Lokální sítě, Wi-Fi ani provozní síť skladů neřeší.

Topologie hub-spoke a adresní plán, region Germany West Central, rezerva 10.60.0.0/16



Plné čáry: peering spoku s hubem, veškerý provoz jde přes firewall. Čárkované: tunely VPN.

- Podsítě spoků mají výchozí trasu na firewall a vypnuté šíření tras z brány. GatewaySubnet posílá rozsahy spoků také přes firewall, takže kontrolou prochází i provoz z lokalit.
- Spoky mezi sebou nemají peering a produkce s testem se nevidí. Povolené jsou jen konkrétní toky, například integrační vrstva do API skladového systému.
- Odchozí provoz jen na povolené FQDN a Azure Monitor. DNS proxy na firewallu je nutná, jinak nefungují FQDN v síťových pravidlech.
- Služby PaaS v corp jen přes privátní endpoint, v online totéž pro data. Záznamy v zónách privatelink.* zakládá politika, lokality předávají tyto zóny na příchozí endpoint resolveru.
- ExpressRoute ani placená ochrana DDoS se v první fázi nenasazují. Brána ExpressRoute jde později přidat bez změny spoků.

5.1 Politiky

Landing zóny vznikají prázdné, proto zakazující pravidla jdou rovnou do vynucení. Výjimka je v kódu s odůvodněním a datem konce.

Pravidlo	Efekt	Rozsah
Regiony jen Germany West Central a West Europe	Deny	org
Sedm povinných tagů na skupinách prostředků	Deny	org
Povinné tagy na prostředcích, píše je kód	Audit	org
Diagnostika kategorie audit do Log Analytics	DeployIfNotExists	org
Microsoft cloud security benchmark	Audit	org
Plány Defender for Cloud, zapíná je kód	AuditIfNotExists	org
Zákaz veřejných IP adres	Deny	corp
Síťové rozhraní bez veřejné IP	Deny	landingzones
Veřejný přístup ke službám PaaS vypnutý	Deny · Audit	corp · online
Záznamy endpointů v zónách privatelink.*	DeployIfNotExists	landingzones
Správcovské porty z internetu v NSG	Deny	org
Podsíť bez NSG	AuditIfNotExists	landingzones
Key Vault s ochranou proti smazání a modelem RBAC	Deny	org
Úložiště bez přístupu sdíleným klíčem	Audit	org
Zálohování virtuálních serverů	AuditIfNotExists	landingzones, identity
Zákaz síťových bran a peeringu	Deny	sandbox
Zákaz nových prostředků	Deny	decommissioned

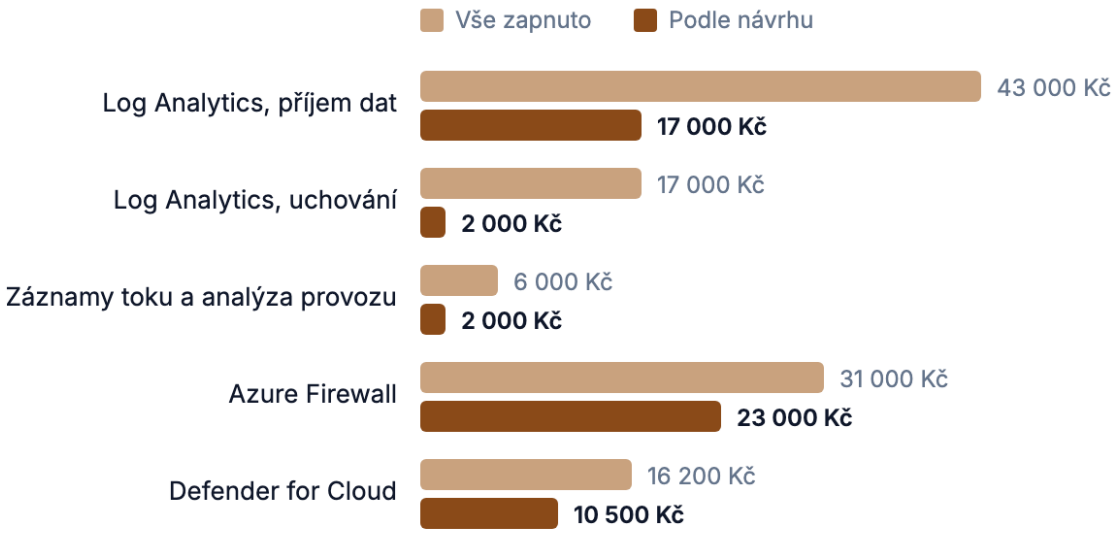
5.2 Diagnostika, výstrahy a zámky

- Protokol aktivit, protokoly Entra ID a kategorie audit jdou do jednoho pracovního prostoru. Záznamy toku jsou VNet flow logs, nové NSG flow logs nejde od 30. 6. 2025 založit.
- Výstrahy hlásí přihlášení nouzového účtu, přidělení privilegované role, změny politik, zámků a diagnostiky mimo pipeline a přístup ke stavu Terraformu jinou identitou.
- CanNotDelete je na prostředcích platformy, ne na skupině prostředků: tam by Azure bránil mazat historii nasazení a po limitu 800 by další nasazení selhávala.

6. Náklady a model nasazení

Srovnání dvou způsobů, jak zapnout tutéž ochranu a dohled: vše naplno ve výchozím nastavení, nebo podle návrhu. Návrh neztrácí žádný záznam, ze kterého čte detekce, výstraha nebo vyšetřování.

Orientační měsíční náklad na ochranu a dohled (Kč bez DPH)



- Příjem: 8 GB denně v analytickém plánu a 5 GB v levnějším plánu Basic místo 22 GB. Do Basic jdou data, ze kterých čte jen vyšetřování, pokud to tabulka podporuje.
- Uchování 90 dní interaktivně a pak dlouhodobě do roku. Analýza provozu jen pro hub a produkci po 60 minutách. Firewall Standard místo Premium (ADR-02).
- Defender for Servers Plan 2 jen v produkci a na řadičích domény (sledování integrity souborů, skenování bez agenta), v testu Plan 1. CSPM a plány PaaS jen v produkci a platformě.
- Nešetří se na protokolech Entra ID, protokolu aktivit, Key Vault a přístupech ke stavu. Mají malý objem a stojí na nich vyšetřování.
- Sedm povinných tagů (app, env, owner, costCenter, criticality, dataClassification, managedBy) píše kód, v Cost Management je zapnuté dědění tagů. Každé předplatné má rozpočet s výstrahami.

> Orientační odhad bez DPH podle veřejného ceníku a objemu z workshopů; ověří se po prvním měsíci provozu. Síťové poplatky a náklady aplikací zahrnuté nejsou.

6.1 Hranice mezi nástroji

Rozhoduje API. Co se zapisuje přes Azure Resource Manager, dělá Terraform s Terragruntem, i když se to týká identity. Co je za Microsoft Graph a rozhraními Microsoft 365, dělá Microsoft365DSC; nic se nenastavuje na dvou místech.

Oblast	Rozhraní	Nástroj
Management groups a zařazení předplatných	Resource Manager	Terraform / Terragrunt
Politiky, iniciativy a výjimky	Resource Manager	Terraform / Terragrunt
Přiřazení rolí Azure skupinám a identitám	Resource Manager	Terraform / Terragrunt
Síť, DNS, firewall a jeho pravidla	Resource Manager	Terraform / Terragrunt
Diagnostika, výstrahy, rozpočty, tagy	Resource Manager	Terraform / Terragrunt
Plány Defender for Cloud	Resource Manager	Terraform / Terragrunt
Záznamy DNS privátních endpointů	Resource Manager	Azure Policy z Terraformu
Skupiny Entra ID a jejich členství	Microsoft Graph	Microsoft365DSC
Role Entra ID, PIM pro role a skupiny, Conditional Access	Microsoft Graph	Microsoft365DSC
Intune, Defender XDR, Purview (mimo návrh)	Graph, PowerShell	Microsoft365DSC

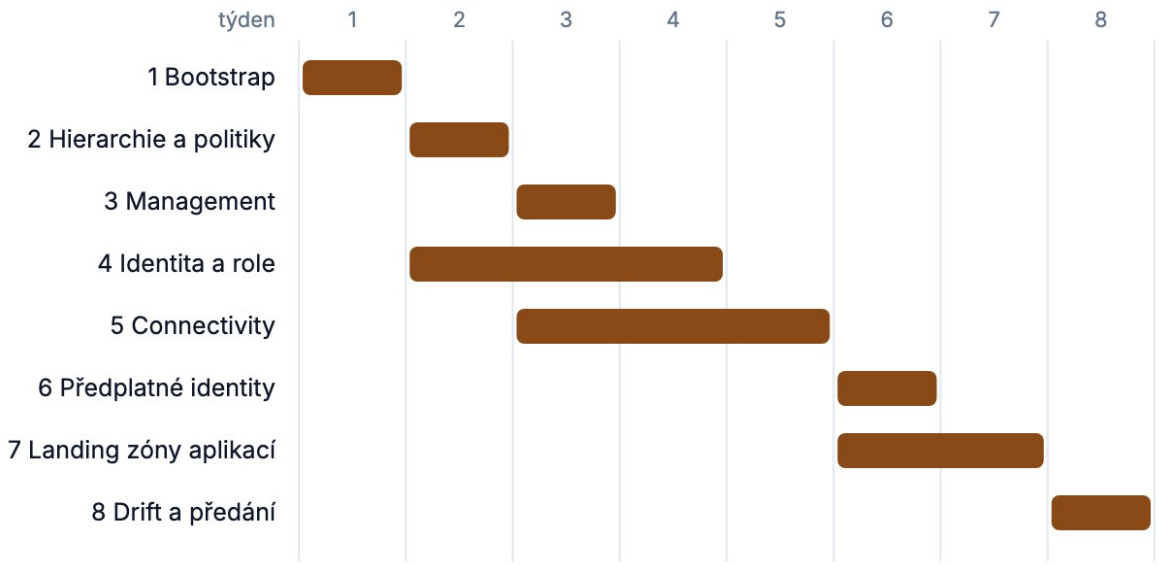
6.2 Tok změny

- Do main jen pull requestem, který schvaluje vlastník kódu podle CODEOWNERS, nikdy autor. Kontroly: formát, validace, tflint, Checkov nebo Trivy, gitleaks a plan.
- Apply čeká na schválení v prostředí prod a kdo nasazení spustil, schválit nesmí. Schvalovatelé prostředí jdou v privátním repozitáři jen v GitHub Enterprise.
- Každou noc běží plan nad celým stromem a nenulový plán jde jako výstraha driftu. Havarijní ruční změna se do jednoho pracovního dne dopíše do kódu.
- Stav je v účtu úložiště s ověřením jen přes Entra ID, verzováním a zámkem CanNotDelete. Runnery GitHubu nemají pevné adresy, proto se místo síťového omezení hlídá přístup (otevřený bod 8).
- Bootstrap spouští člověk s rolí Owner aktivovanou v PIM: kořen org, identity pipeline, vlastní role, privilegovaná přiřazení, účet se stavem a export protokolů Entra ID.

7. Roadmapa a rozhodnutí

Pořadí kroků stojí na závislostech. Pracnost platí pro tým, který zná Terraform a Azure, a nezahrnuje migraci aplikací.

Harmonogram (týdny)



Krok	Obsah	Závisí na	Pracnost
1	Bootstrap: kořen org, identity pipeline, vlastní role, stav, nouzové účty, export protokolů Entra ID	—	Nízká
2	Hierarchie, zařazení předplatných, politiky, plány Defender for Cloud	1	Střední
3	Management: Log Analytics, diagnostika, výstrahy, rozpočty	2	Nízká
4	Identita: skupiny, role Entra ID a PIM, správcovské účty, Conditional Access pro správce	1, obsazení rolí	Vysoká
5	Connectivity: hub, firewall a pravidla, VPN do tří lokalit, DNS resolver, privátní zóny	2, správce sítě	Vysoká
6	Předplatné identity: řadiče domény v Azure, přesun Entra Connect	4, 5	Střední
7	Landing zóny tří aplikací: šest předplatných, spoky, role, rozpočty	3, 5	Střední
8	Noční drift, provozní postupy, předání týmu	7	Nízká

7.1 Zaznamenaná rozhodnutí

Rozhodnutí	Zamítnuté varianty	Proč
ADR-01 Síť hub-spoke s Azure Firewall	Virtual WAN; FortiGate v Azure	jeden region, tři lokality, žádný tranzit mezi pobočkami; nejnižší cena a pravidla v kódu. Při druhém regionu přechod na Virtual WAN
ADR-02 Azure Firewall Standard	Premium; Basic	Basic má omezenou propustnost. IDPS a inspekci TLS z Premium odchozí provoz jen na povolené FQDN zatím nevyužije, rozdíl je kolem 8 000 Kč měsíčně
ADR-03 Hranice produkce a testu je předplatné	management group na prostředí; jedno předplatné na aplikaci	stejné politiky v obou prostředích, oddělené přístupy, rozpočty a síť
ADR-04 Pipeline přes spravovanou identitu s federací	registrace aplikace s certifikátem nebo s federací	žádné tajemství; spravované identitě nejde přidat heslo ani certifikát
ADR-05 Jeden bezpečnostní pracovní prostor	jeden prostor pro vše; prostor na předplatné	Sentinel se platí za data v prostoru, provozní telemetrie by ho prodražila; jedno místo pro vyšetřování
ADR-06 DNS přes Private Resolver a DNS proxy firewallu	řadiče domény jako DNS pro Azure; vlastní DNS servery	řadiče domény by se staly závislostí každé aplikace; resolver je spravovaná služba

8. Přílohy

8.1 Strojově čitelný výstup

Návrh se předává jako repozitář, ne jako obrázek. Adresářový strom kopíruje hierarchii, soubory .hcl nesou kontext a každá jednotka má kompletní vstupy; vedle je konfigurace Microsoft365DSC.

mg-landingzones/mg-corp/sub-wms-prod/gwc/rg-app/key-vault/terragrunt.hcl, výřez

```
inputs = {
  purge_protection_enabled = true
  public_network_access    = false
  private_endpoint = { subnet = "snet-pep-wms-prod-gwc-001" }

  # povinné vstupy každého modulu, bez výchozích hodnot
  diagnostics = include.root.locals.diagnostics_security
  alerts      = { availability = { threshold = 99.9 } }
  lock        = "CanNotDelete"
  role_assignments = {
    "Key Vault Secrets User"  = ["id-wms-app-prod"]
    "Key Vault Administrator" = ["sg-az-wms-prod-ops"]
  }
}
```

Jednotka bez diagnostiky, výstrah, zámku nebo přístupů neprojde ani plánem a vypnutí se píše výslovně. Členství ve skupině správců je oprávněné v PIM a záznam v privátní DNS zóně doplní politika.

8.2 Otevřené body

Bod	Otázka	Na čem závisí
1	Pořídit Defender for Identity, který E3 nezahrnuje, nebo spoléhat na záznamy serverů?	detekce útoků na doménu
2	Entra ID P2 pro dalších přibližně deset lidí?	oprávněné role v PIM
3	Přihlašovat správce jen z vyhrazených stanic pro správu?	Conditional Access
4	Vyžaduje předpis nebo pojišťovna inspekci TLS a IDPS?	ADR-02, cena firewallu
5	Placená ochrana DDoS pro veřejné vstupy portálu a integrace?	náklady, volba WAF
6	Jak dlouho uchovávat záznamy podle předpisů a regulace?	retence a její cena
7	Cíle obnovy (RPO a RTO) skladového systému?	zálohy v jednom regionu
8	Síťově omezit účet se stavem, například runnery v síti organizace?	provoz a cena pipeline