Přechod na doménu identita.gov.cz

Hlavním cílem projektu je přechod ze stávající domény identitaobcana.cz na doménu identita.gov.cz.

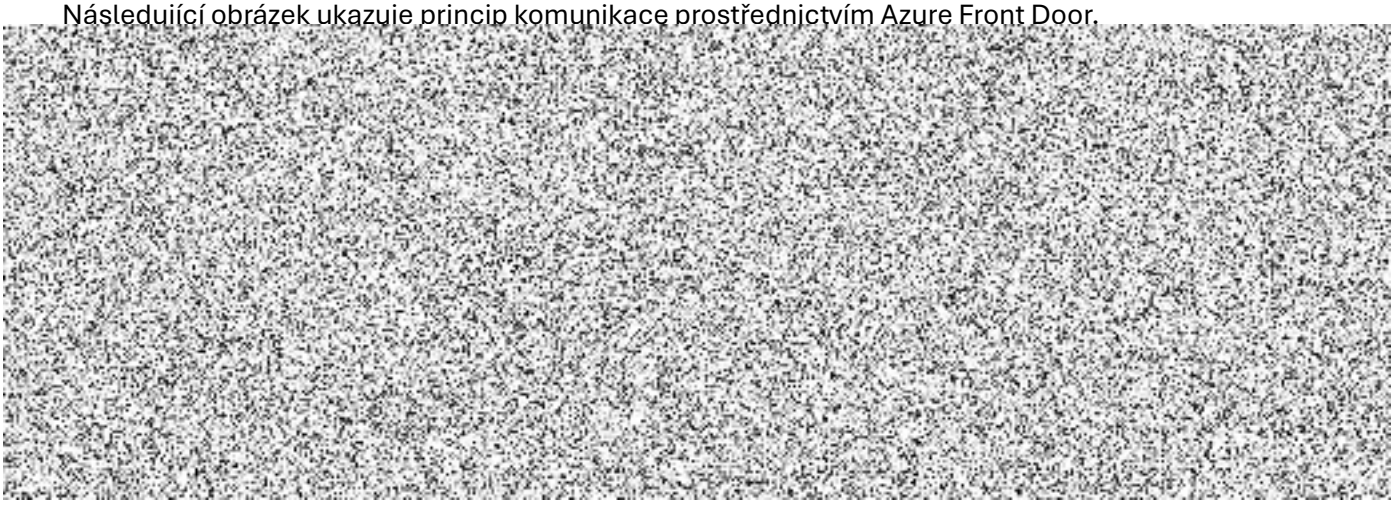
Doplňkovým cílem je, aby komunikace do prostředí NIA probíhala prostřednictvím Azure Front Door (AFD), který umožní:

- Zakončení komunikace IPv4 a IPv6 a následná komunikace do prostředí CMS a NIA bude probíhat na protokolu IPv4. Tím se zajistí, že při přepínání provozu mezi datovými centry nebude nutné provádět ruční přepínání DNS pro IPv6.
- Vkládání hlaviček do http protokolu, zvláště pak informaci o IP adrese uživatele. V současné době toto CMS a F5 nedělá, a proto se informace o IP adrese uživatele ztrácí. To znamená, že v logovacích databázích se nacházejí IP adresy F5.

Po přechodnou dobu musí být funkční obě domény a musí umožnit paralelní provoz.

Princip komunikace s využitím AFD

Následující obrázek ukazuje princip komunikace prostřednictvím Azure Front Door.



1. ~~1.~~Uživatel v prohlížeči zadá požadovanou URL adresu. Např. https://twww.identita.gov.cz anebo https://twww.identitaobcana.cz.
2. Požadavek je směrován na AFD endpoint dle CNAME záznamu v DNS. Podle konfigurace počítače uživatele se použije protokol IPv4 anebo IPv6.
3. AFD dle konfigurace využije Endpoint, Route, Origin group a Origin.
4. AFD naváže komunikaci se serverem NIA prostřednictvím technické domény. Např. https://twww-tech.servicesnia.net. Tato technická doména slouží k otevření TLS komunikace mezi AFD a IIS. Následně AFD pošle požadavek v otevřeném TLS kanálu pro doménu https://twww.identitaobcana.cz. Komunikace půjde stávající prostřednictvím CMS a nakonfigurovaných F5 prostřednictvím IPv4. AFD do požadavků vloží všechny požadované hlavičky vč. originální IP adresy uživatele.

Konfigurace Azure Front Door (AFD)

Doménová jména

V prostředí AFD bude nutné provést registraci všech domén, které se momentálně pro komunikaci s NIA používají. Následující tabulky obsahují přehled doménových jmen a současné IP adresy.

Pro komunikace mezi AFD a datovými centry jsou vyžadovány technické domény, aby bylo možné provést směrování provozu z AFD do datového centra.

Vyřešit domény, které nebudou přecházet na novou doménu např. eOP Middleware, které by také měly přejít na komunikaci přes AFD. Přechod je nutný z důvodu řízení přepínání IPv6.

Testovací prostředí

Stávající doména	Nová doména	Technická doména	IP adresa
tnia.identitaobcana.cz	tnia.identita.gov.cz	tnia-tech.servicesnia.net	
tma.identitaobcana.cz	tma.identita.gov.cz	tma-tech.servicesnia.net	
teop.identitaobcana.cz	teop.identita.gov.cz	teop-tech.servicesnia.net	
twww.identitaobcana.cz	twww.identita.gov.cz	twww-tech.servicesnia.net	
tsms.identitaobcana.cz	tsms.identita.gov.cz		
tmweop.identitaobcana.cz	tmweop.identita.gov.cz	tmweop-tech.servicesnia.net	
tinternal.identitaobcana.cz	tinternal.identita.gov.cz	Není potřeba	
tautorizace.narodnibod.cz	tautorizace.identita.gov.cz	taut-tech.servicesnia.net	
tovereni.identitaobcana.cz	tovereni.identita.gov.cz	twww-tech.servicesnia.net	
toverenimeg.identitaobcana.cz	toverenimeg.identita.gov.cz	twww-tech.servicesnia.net	
tnia.narodnibod.cz	tnia.identita.gov.cz	tnia-tech.servicesnia.net	

Produkční prostředí

Stávající doména	Nová doména	Technická doména	IP adresa
identitaobcana.cz	identita.gov.cz	www-tech.servicesnia.net	
nia.identitaobcana.cz	nia.identita.gov.cz	nia-tech.servicesnia.net	
ma.identitaobcana.cz	ma.identita.gov.cz	nia-tech.servicesnia.net	
eop.identitaobcana.cz	eop.identita.gov.cz	eop-tech.servicesnia.net	
www.identitaobcana.cz	www.identita.gov.cz	www-tech.servicesnia.net	
sms.identitaobcana.cz	sms.identita.gov.cz	sms-tech.servicesnia.net	
mweop.identitaobcana.cz	mweop.identita.gov.cz	mweop-tech.servicesnia.net	
internal.identitaobcana.cz	internal.identita.gov.cz	Není potřeba	
autorizace.narodnibod.cz	autorizace.identita.gov.cz	autorizace-tech.servicesnia.net	
overeni.identitaobcana.cz	overeni.identita.gov.cz	www-tech.servicesnia.net	
overenimeg.identitaobcana.cz	overenimeg.identita.gov.cz	www-tech.servicesnia.net	
reporting.identitaobcana.cz	reporting.identita.gov.cz	Není potřeba	
narodnibod.cz	identita.gov.cz	www-tech.servicesnia.net	

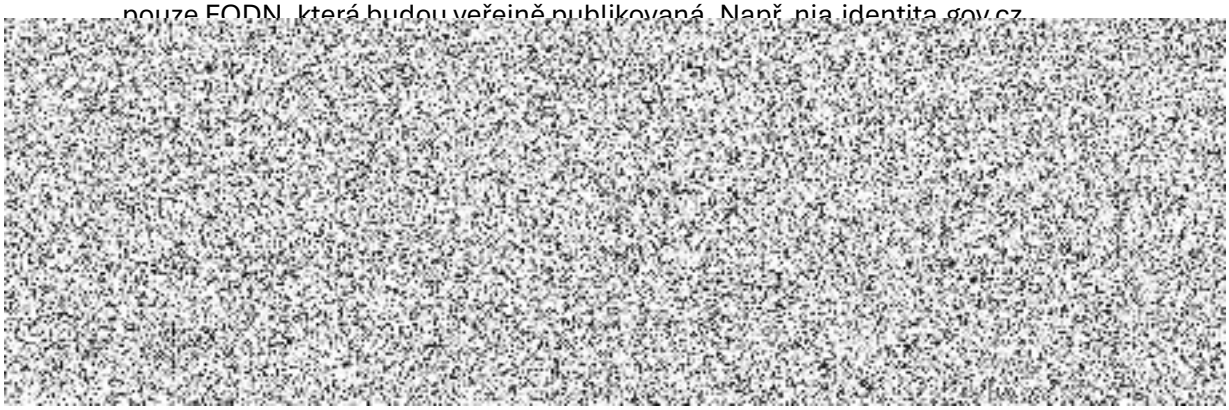
Testovací adresy produkčního prostředí

Testovací adresy produkčního prostředí nebudou využívány přes AFD.

Certifikáty

Konfigurace bude vyžadovat vydání nových certifikátů a bude nutné mít pro každé prostředí dvě sady certifikátů.

- Certifikát pro AFD, který bude umístění v Azure Key Vault. Tento certifikát bude obsahovat pouze FQDN, která budou veřejně publikovaná. Např. nia.identita.gov.cz



- Certifikát pro IIS, který bude nainstalovaný na všech GG-IIS a Portal serverech. Tento certifikát musí umožnit příjem komunikace na technické doméně. Doporučujeme použít tzv. wildcard certifikát. V případě, že wildcard certifikát nebude použit, pak v Alternative Names musí být uvedeny FQDN nové domény a zároveň FQDN technických domén.

Požadované certifikáty

FQDN	Poznámka
*.narodnibod.cz	Certifikát je vydaný a platný do 25.6.2025. Bude použit pro komunikaci s AFD. Bude muset být nainstalovaný v AFD. Certifikát je použit pro testovací i produkční prostředí. Certifikát bez Alternative names
*.servicesnia.net	Nově vydaný certifikát Technický certifikát pro komunikaci mezi AFD a servery v datových centrech Vápenka a Malešice. Certifikát bez Alternative names. Certifikát je ryze technický a doporučujeme ho vydat s delší platností než 1 rok.
*.identita.gov.cz	Nově vydaný certifikát Bude použit pro komunikaci s AFD. Bude muset být nainstalovaný v AFD. Certifikát je použit pro testovací i produkční prostředí. Certifikát bez Alternative names.

*.identitaobcana.cz	Stávající certifikát, který po expiraci nebude obnoven Bude použit pro komunikaci s AFD. Bude muset být nainstalovaný v AFD. Certifikát je použit pro testovací i produkční prostředí. Certifikát bez Alternative names.

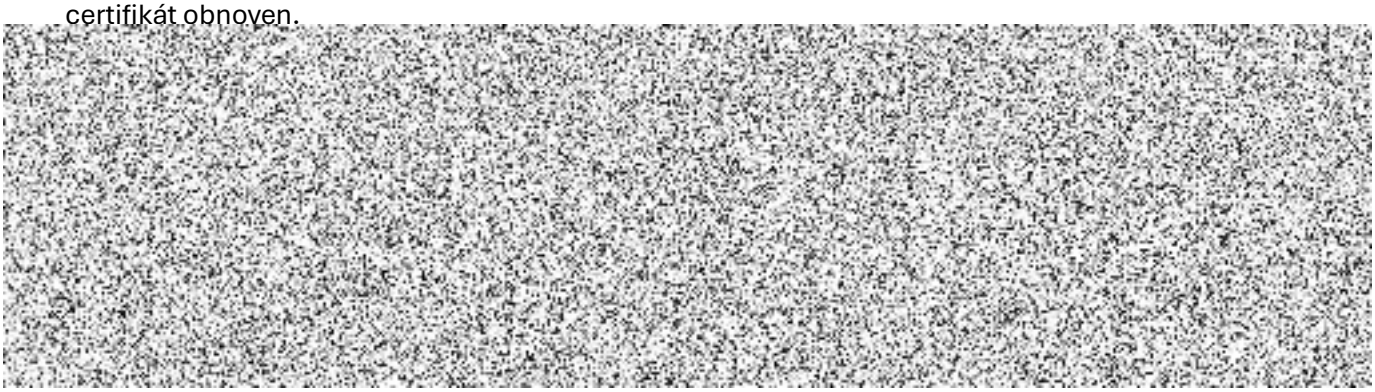
Obnova certifikátů

Certifikáty se po obnově musí aktualizovat na dvou místech:

1. Azure Key Vault
2. Příslušné IIS servery

Rotace certifikátů v Azure Front Door

Certifikát uložený Azure Key Vault musí být v AFD přidaný jako Secret. Pokud se při přidávání certifikátu jako Secret zvolí parametr „Latest“, AFD automaticky obnoví certifikát, kdykoliv je certifikát obnoven.

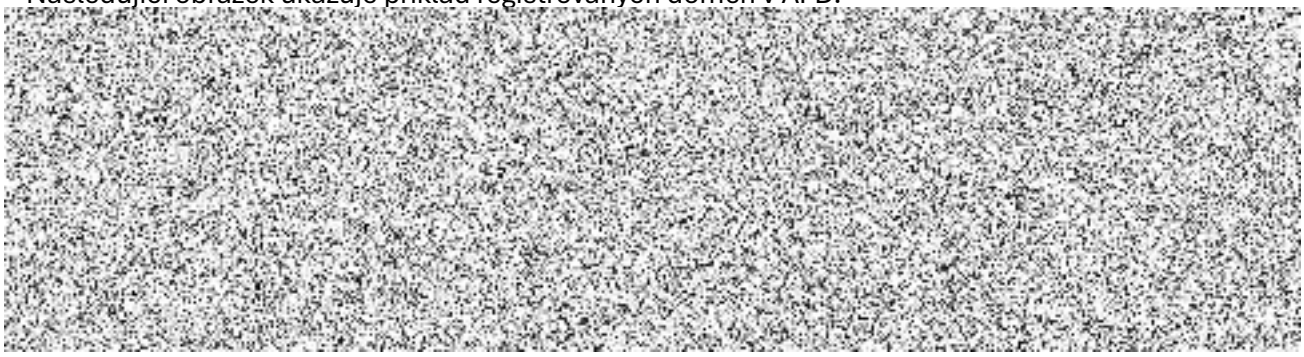


Rotace certifikátů na IIS

Rotace certifikátů na IIS bude probíhat dle stávajících postupů.

Registrace domén v AFD

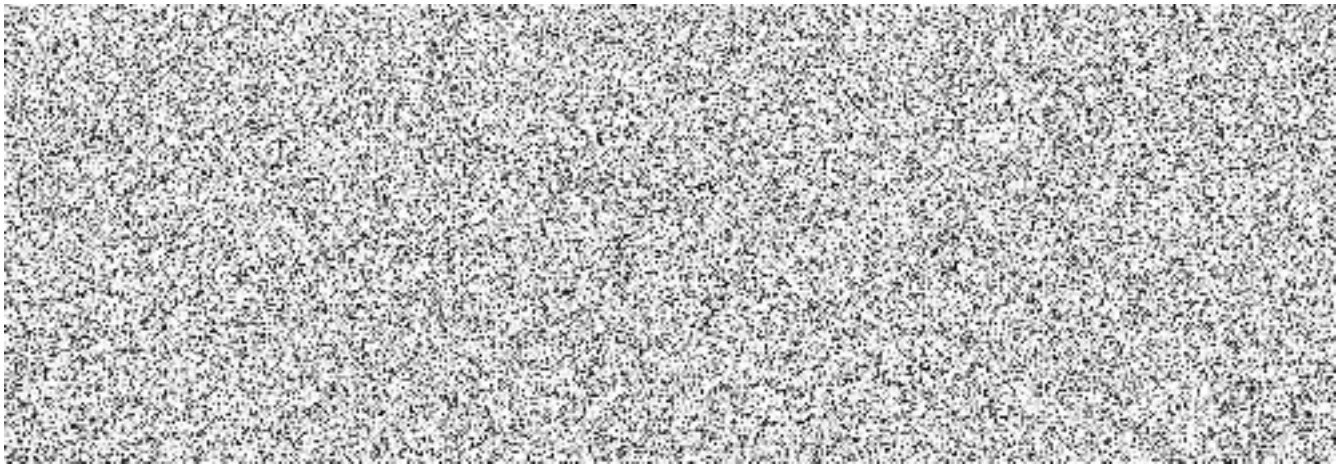
Každá z výše uvedených domén bude v AFD zaregistrována a bude k ní přiřazen vydaný certifikát. Následující obrázek ukazuje příklad registrovaných domén v AFD.



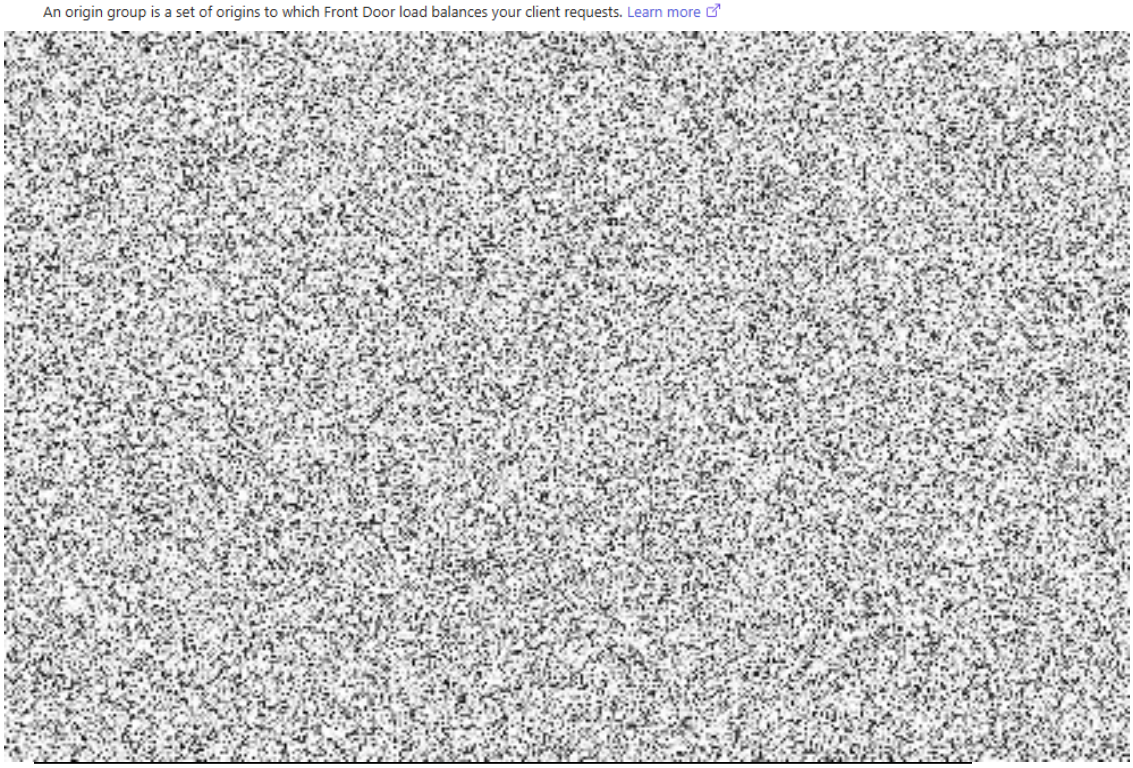
Registrace domén bude vyžadovat spolupráci se správci domény identita.gov.cz, aby bylo možné provést validaci domény. Dále bude nutné provést registraci CNAME záznamů pro všechny uvedené domény.

Registrace Origin groups

Origin groups slouží pro konfiguraci směrování provozu na konkrétní koncové body vlastních aplikací.

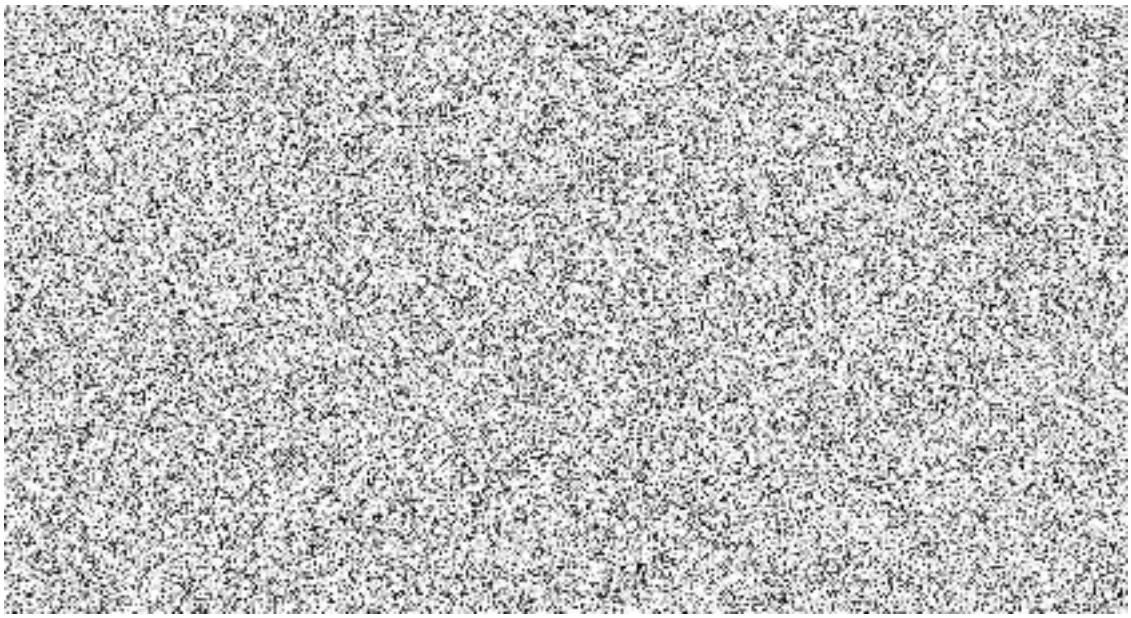


Pro každou registrovanou doménu, resp. společnou technickou doménu bude vytvořena příslušná Origin group, která bude obsahovat konfiguraci jedné origin.



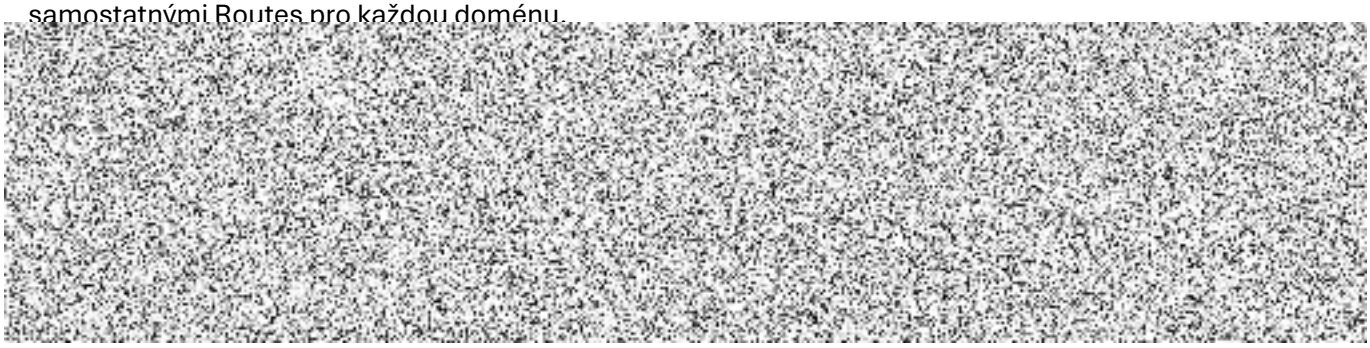
Bude provedena konfigurace origin tak, aby odkazovala na příslušnou technickou doménu.

Origins are your application servers. Front Door will route your client requests to origins, based on the type, ports, priority, and weight you specify here. Learn more



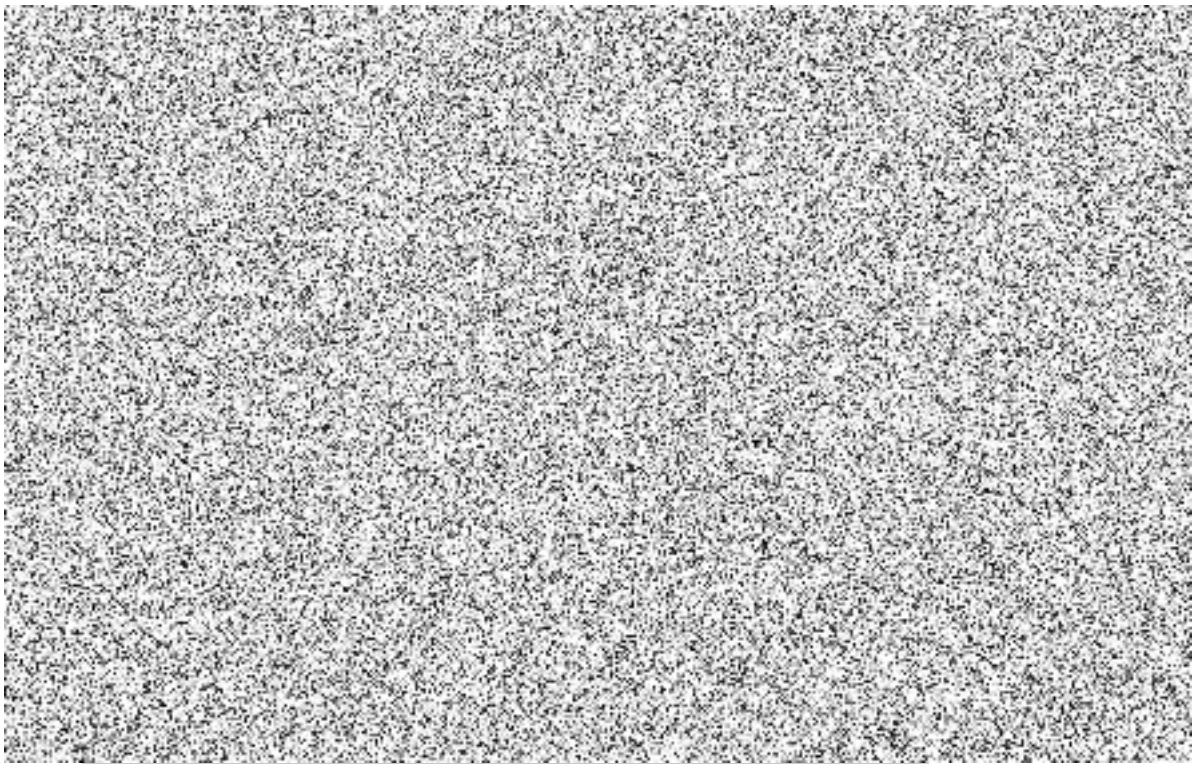
Konfigurace AFD Endpoint

Azure Front Door endpoint je definován jménem subdomény, která je vytvořena pod výchozí doménou AFD (např. .z02.azurefd.net) a slouží pro směrování provozu z klienta na definované koncové body. Na takto vytvořený endpoint jsou směrovány CNAME záznamy pro vlastní definované domény. Pro každý endpoint se konfigurují Routes, které mapují vstupní doménu a další parametry s konkrétním Origin group. Následující obrázek ukazuje příklad konfigurovaného endpointu se samostatnými Routes pro každou doménu.



Konfigurace route

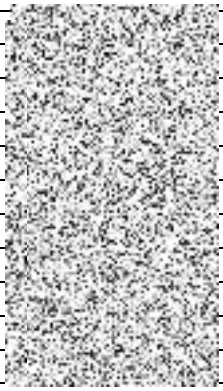
Každá route slouží pro definici mapování mezi vstupní doménou, protokolem a dalšími parametry s vybranou Origin group. Následující obrázek ukazuje příklad definice route.



Konfigurace DNS

Pro změny komunikace bude nutné provést následující změny DNS záznamů

Doména	Typ záznamu	Hodnota
identitaobcana.cz nia.identitaobcana.cz ma.identitaobcana.cz eop.identitaobcana.cz www.identitaobcana.cz sms.identitaobcana.cz mweop.identitaobcana.cz internal.identitaobcana.cz autorizace.narodnibod.cz overeni.identitaobcana.cz overenimeg.identitaobcana.cz narodnibod.cz identita.gov.cz nia.identita.gov.cz ma.identita.gov.cz eop.identita.gov.cz www.identita.gov.cz sms.identita.gov.cz mweop.identita.gov.cz internal.identita.gov.cz autorizace.narodnibod.cz overeni.identita.gov.cz overenimeg.identita.gov.cz	CNAME	nia-dcs-gkcuaeffbuaxe0ad.a02.azurefd.net

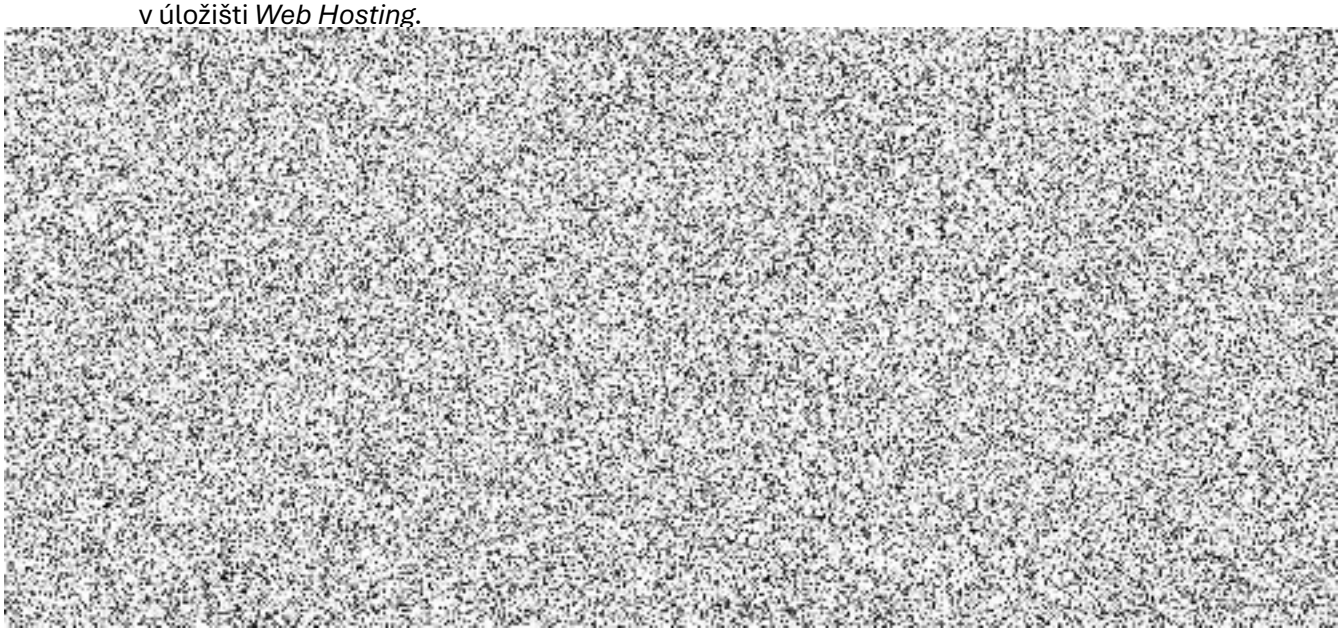
tnia.identitaobcana.cz tma.identitaobcana.cz teop.identitaobcana.cz twww.identitaobcana.cz tsms.identitaobcana.cz tmweop.identitaobcana.cz tinternal.identitaobcana.cz tautorizace.narodnibod.cz tovereni.identitaobcana.cz toverenimeg.identitaobcana.cz tnia.identita.gov.cz tma.identita.gov.cz teop.identita.gov.cz twww.identita.gov.cz tsms.identita.gov.cz tmweop.identita.gov.cz tinternal.identita.gov.cz tautorizace.narodnibod.cz tovereni.identita.gov.cz toverenimeg.identita.gov.cz	CNAME	nia-dcs-gkcuaeffbuaxe0ad.a02.azurefd.net
tnia-tech.servicesnia.net	A	
teop-tech.servicesnia.net	A	
twww-tech.servicesnia.net	A	
tmweop-tech.servicesnia.net	A	
taut-tech.servicesnia.net	A	
www-tech.servicesnia.net	A	
nia-tech.servicesnia.net	A	
eop-tech.servicesnia.net	A	
sms-tech.servicesnia.net	A	
mweop-tech.servicesnia.net	A	
autorizace-tech.servicesnia.net	A	

Konfigurace IIS v datových centrech

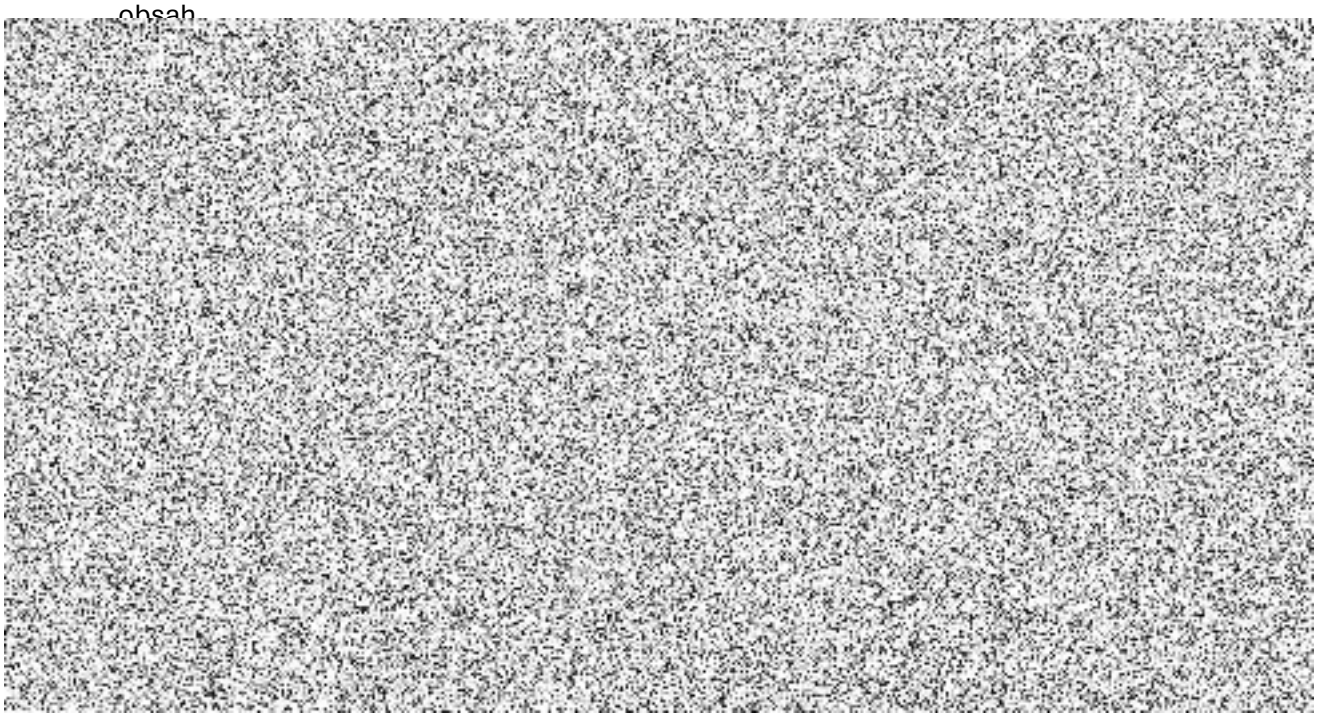
Konfigurace budu provedeny na všech GG-IIS, PORTAL a MWEOP serverech.

Pro komunikaci mezi AFD a origin a IIS je použitá technická doména. Komunikace probíhá prostřednictvím TLS protokolu, a proto je nutné:

1. Provést import certifikátu, který je vydaný pro technickou doménu. Certifikát bude uložený v úložišti *Web Hosting*.



2. Bude vytvořená nová IIS site *TechEndpoint*, která bude mít vytvořený SSL binding pro všechny IP adresy a bude mít nastavený certifikát technické domény. Site nebude mít žádný obsah.



Konfigurace prostředí NIA pro novou doménu

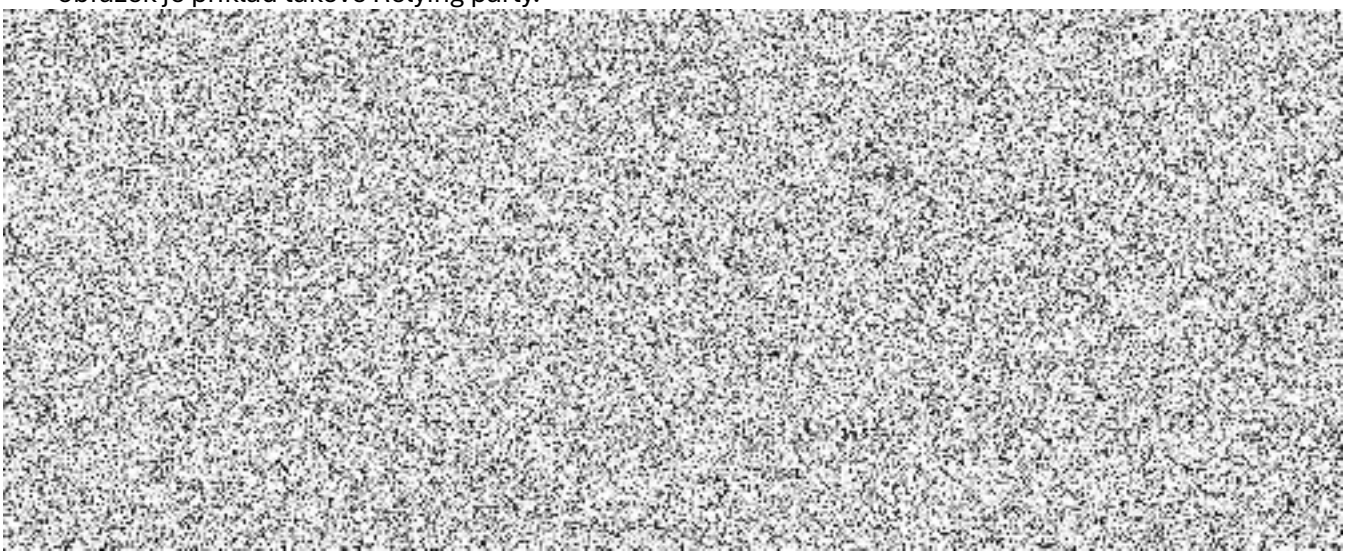
Příslušné konfigurace NIA budou muset být upraveny tak, aby pracovali s novou doménou:

1. Úpravy konfigurací vybraných Trusted Relying parties
2. Úpravy konfigurací všech komponent, které používají doménu identitaobcana.cz

3. Úpravy konfigurací IP adres a domén v souboru hosts
4. Úpravy konfigurace interní DNS

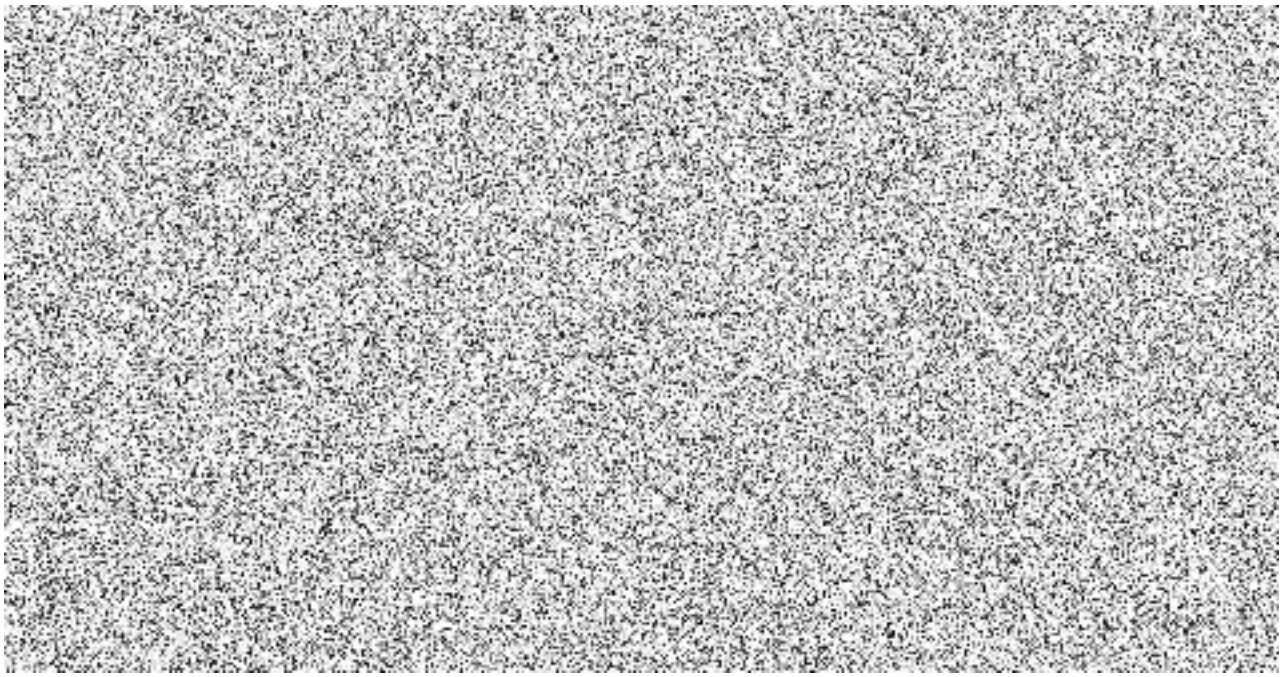
Trusted Relying parties

Budou upraveny konfigurace všech Trusted Relying parties, které jsou závislé na doménových jménech. Jedná se primárně o ty, které potřebují mít nastavený parametr AppliesTo. Následující obrázek je příklad takové Relying party.



Konfigurace komponent

Konfigurace komponent se provedou v CGGConfiguration, kde budou záznamy buď přepsány anebo budou do konfigurace přidány záznamy o nové doméně tak, aby byl zajištěn souběh domén. Následující obrázek ukazuje příklad konfiguračních záznamů.



Konfigurace IP adres a domén v souboru hosts

Pro řadu komunikací se využívají záznamy v souboru hosts, které zajišťují, že se pro danou doménu rozpoznávají IP adresy požadovaného serveru pro případy, kdy není žádoucí mít odpověď z interního DNS serveru. Např. pro zajištění, že následná komunikace z IIS serveru bude směrována na ten samý IIS server, a nikoliv na jiný ve farmě. Tyto typy volání mají eliminovat nežádoucí síťový provoz.

Úpravy konfigurace interní DNS

V interním DNS serveru budou přidány záznamy pro novou doménu a tyto záznamy budou směrovat na vstupní IP adresu F5, která zajišťuje komunikaci s IIS servery GG a Portálu.

Souběh doménových jmen

Po přechodnou dobu bude podporován souběh doménových jmen. Z pohledu interakcí s NIA existují dva typy komunikací:

1. Prostřednictvím prohlížeče
2. Prostřednictvím webových služeb

Komunikace prostřednictvím prohlížeče

Klíčovou komponentou pro komunikaci s prostřednictvím prohlížeče je Federation provider a NIA Identity providers, které vyžadují, aby komunikace probíhala na „správné“ nové doméně. V případě, že přijde požadavek na původní doménu, provede Federation provider přesměrování na novou doménu. Tento opravný mechanismus je funkční pouze při komunikaci mezi SePem a NIA. V praxi to znamená, že SeP může poslat na NIA požadavek na přihlášení na starou doménu. NIA pak následně provede přesměrování na novou doménu.

Pro poskytovatele identit tento opravný mechanismus není možné použít (viz. kapitola Publikovaná metadata).

Komunikace prostřednictvím webových služeb

Komunikace prostřednictvím webových služeb není přímo závislá na doménovém jméně. Tato komunikace se primární týká externích subjektů z pohledu NIA, jako banky anebo ISZR. Tyto systémy mají nastavené adresy na volání webových služeb. Souběh bude funkční na původní doméně až do doby, kdy dojde k expiraci certifikátu s původní doménou anebo kdy bude původní doména odebrána z konfigurace webových serverů.

Publikovaná metadata

Po konfiguraci nové domény v centrální konfiguraci NIA, kde se nová doména stane primární, začne NIA publikovat metadata s novou doménou. Tato změna je důležitá primárně pro externí poskytovatele identit, kdy jejich konfigurace musí na tuto změnu reagovat a musí začít odesílat odpovědi o přihlášení na nové adresy. Změna musí být s poskytovateli identit včas projednána, protože může nastat situace, kdy systémy poskytovatelů identit na metadata nereagují anebo pouze v určitých časových intervalech.

Poskytovatelé služeb (SeP) by se také měly řídit publikovanými metadaty a jejich systémy by se měly automaticky přizpůsobit a zasílat požadavky na novou doménu. V případě, že se metadaty neřídí musí provést manuální změnu na své straně. Tato změna není z pohledu NIA časově kritická, protože NIA po přechodnou dobu bude pro tyto komunikace provádět automatické přesměrování na novou doménu.