ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ - ÚSEK INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ
Křížová 25, 225 08 Praha 5

Standard systému Active Directory, DNS, DHCP, NTP

Verze 1.33

Změny:

Datum vydání	Verze	Změna proti předchozí verzi	Změnil (jméno)
8.2.2005	0.80	První draft	Libor Šmíd
29.6.2006	1.00	Úprava do finální verze	Milan Zapletal, Jan Boháč
19.7.2006	1.10	Dopracování služby NTP	Milan Zapletal
9.8.2006	1.20	Dopracování PKI	Libor Šmíd
11.12.2006	1.32	Úpravy NTP, DNS, doplnění domény app.cssz.cz	Libor Šmíd
21.12.2006	1.33	Doplnění syntaxe DNS pro db.cssz.cz	Libor šmíd
18.6.2008	1.34	Změny v DNS	Zapletal

Obsah

1. ÚVOD 3

2. ACTIVE DIRECTORY 3
2.1 Active Directory cssz.cz 3
2.1.1 Struktura Active Directory 4
2.1.2 Group Policy 4
2.2 Active Directory app.cssz.cz 5
2.2.1 Struktura Active Directory 5
2.2.2 Group Policy 5

3. SLUŽBY DNS 5
3.1 DNS & Active Directory cssz.cz 5
3.1.1 Klientské stanice v doméně cssz.cz 5
3.1.2 Servery v sídle OZZ,KZZ 6
3.1.3 Servery v sídle UXX a APP 6
3.1.4 Jmenná syntaxe 6
3.2 DNS & Active Directory app.cssz.cz 6
3.2.1 Jmenná syntaxe 6
3.3 DNS & management zóna 8
3.4 DNS & Internet 8

4. SLUŽBY DHCP 9
4.1 Scope 9
4.2 Parametry nastavované prostřednictvím DHCP 12

5. SLUŽBY NTP 13

1. ÚVOD

Standard definuje parametry a strukturu systému Active Directory, DNS a DHCP.

2. ACTIVE DIRECTORY

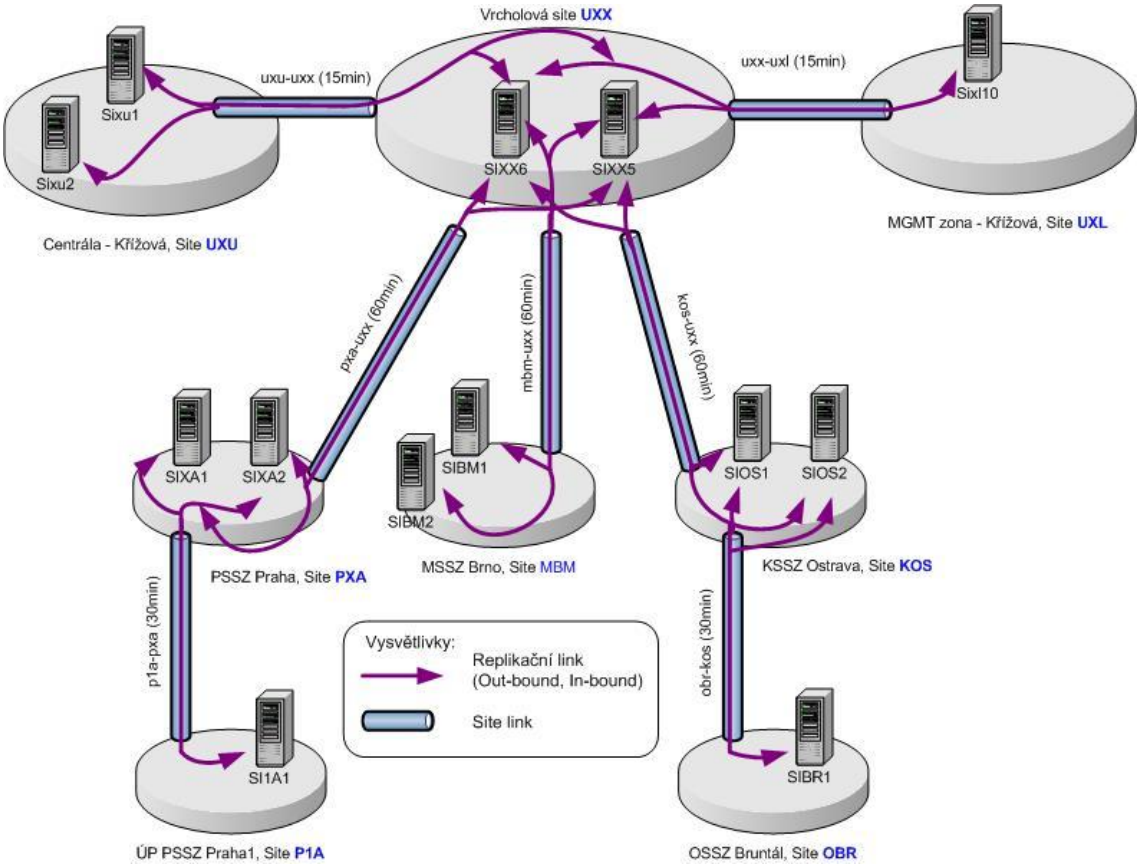
ČSSZ používá dva samostatné foresty, každý s jednou doménou Active Direktory, které nemají navázán mezi s sebou žádný vztah: cssz.cz a app.cssz.cz, Doména cssz.cz je určena k provozu počítačových systémů ve vrstvách infrastrukturních serverů LAN a WAN a LAN UOJ, doména app.cssz.cz je určena k provozu v aplikační vrstvě (viz Standard síťové infrastruktury)

2.1 Active Directory cssz.cz

Doména Active Directory cssz.cz je nastavena v režimu forestu na Windows Server 2003. Doménové servery jsou umístěny po dvou jednak v centrální site, site ústředí a KSSZ, PSSZ a MSSZ, po jednom pak na každé OSSZ.

Pro jednotlivé provozní role Active Directory jsou definováni jak primární vlastníci FSMO rolí, tak sekundární vlastníci, na něž budou v případě výpadku primárního vlastníka příslušné provozní role přesunuty. Přesun rolí sice musí být proveden ručně, avšak je důležité mít definován záložní doménový řadič. Z pohledu běžné funkčnosti jsou nejdůležitější role RID Master a PDC Emulator, v případě rozšiřování schématu ještě role Schema Master. Zbývající role Infrastructure Master a Domain Naming Master nejsou v jednodoménovém modelu využívány, ke slovu by se dostaly pouze v případě, bylo-li by rozhodnuto o vytvoření dceřiné domény v rámci doménové struktury cssz.cz (v rozporu se současným designem).

V rámci domény cssz.cz jsou role FSMO umístěny na doménové řadiče sixx5 a sixx6 v ústředí ČSSZ. V případě výjimečné události nebo při plánovaných odstávkách budou tyto role přesouvány právě mezi těmito servery. Všechny doménové řadiče jsou současně konfigurovány jako globální katalogy. Replikační topologie mezi jednotlivými doménovými řadiči je následující:



2.1.1 Struktura Active Directory

Struktura Active Directory vychází z regionálního uspořádaní ČSSZ. Kromě implicitní struktury kontejnerů /např. kontejnery Builtin, Users atd./ jsou vytvořeny kontejnery /OU/ pro každou lokalitu ČSSZ. Pro pojmenování byla použita tříznaková jmenná konvence, kde první písmeno určuje, zda se jedná o kraj (K) nebo okres (O). Zbylé dva znaky tvoří kód lokality. Výjimkou z této jmenné konvence je pojmenování OU pro Ústředí (U) a PSSZ (P).

Struktura v krajských OU je třívrstvá. V každém krajském OU jsou vytvořeny OU pro okresy spadající územně pod daný kraj. V rámci těchto okresních OU jsou vytvořeny samostatné OU pro objekty počítačů (_Desktopy), skupin (_Skupiny), uživatele (_Uzivatele) a servery (_Servery). Objekty umístěné v těchto OU mohou spravovat místní administrátoři, možnosti správy záleží na delegovaných oprávněních.

Kromě implicitních a krajských OU v Active Directory byly vytvořeny specifické OU pro centrálně spravované objekty, které v pojmenování používají vždy podtržítko (_) + název skupiny. Jde např. o následující OU: _AdminUcty, _Servery.

2.1.2 Group Policy

V rámci Active Directory jsou definovány dvě základní doménové politiky, které se aplikují na všechny objekty v rámci domény cssz.cz. Jde o Default domain policy a Default Domain Controllers Policy, která jsou aplikovány na všechny uživatelské účty, počítače a doménové controllery v rámci organizace. Výjimkou jsou objekty umístěné ve specifických OU /viz.výše/. V Default domain policy a v Default Domain Controllers Policy jsou nastaveny pouze parametry, které jsou akceptovatelné většinou uživatelů, počítačů a doménových controllerů – např. seznam důvěryhodných serverů v Internetu, Password Policy atd.

Kromě defaultních politik existují v rámci krajů a okresů lokální politiky /Lokalita XXX Policy, Domain Controllers XXX Policy/, které modifikují nastavení v rámci kraje nebo okresu. Tyto politiky jsou pak linkovány na patřičná OU.

2.2 Active Directory app.cssz.cz

Doména Active Directory app.cssz.cz je nastavena v režimu forestu na Windows Server 2003. Doménové servery jsou umístěny po jednom v lokalitách KP1 a KP2, přičemž obě lokality představují jedinou site.

Oba doménové řadiče jsou současně konfigurovány jako globální katalogy.

2.2.1 Struktura Active Directory

Navrhovaná struktura OU, administrativních skupin a účtů umožňuje jednoduchým způsobem za předpokladu přítomnosti účtu správce v konkrétní globální skupině správců aplikačních serverů přidělit na požadované servery příslušná oprávnění. Jako výchozí OU je využita OU APP_Management, v které jsou OU Servers, Admins, Grous a Services. OU Admins je dále členeno na OU dle firem (CSSZ, SBS, Microsoft), ostatní OU jsou členěna dle jednotlivých aplikací (NEM, POJ, T-NEM, ...)

2.2.2 Group Policy

Na každou skupinu serverů bude aplikována skupinová politika určující členství ve skupině lokálních administrátorů serverů a ve skupině Remote Desktop Users pro vzdálenou správu serveru.

3. SLUŽBY DNS

3.1 DNS & Active Directory cssz.cz

Vazba mezi jménem a IP adresou počítačů je definována v databázích name serverů, což poskytuje jednodušší možnost přenosu aplikací na IP adresy. V novém doménovém modelu je služba DNS nativní součástí Active Directory, běžící na každém doménovém řadiči SiZZ1 (10.zz.6.10) O správné přidělení IP adresy, DNS a GW stanicím v doméně cssz.cz se stará služba DHCP běžící na stejném serveru. V souladu s filosofií umístění maximálního počtu potřebných služeb co nejblíže uživateli, je služba DNS instalována na každém doménovém řadiči, jinak řečeno v každé lokalitě (Ústředí, KSSZ, PSSZ, MSSZ, OSSZ i ÚP PSSZ). Díky tomu je služba DNS dostupná v každé site Active Directory a většina komunikace při vyhledávání služeb domény *Windows* (příslušnost k site, DC, GC, PDC Emulátor, registrace a deregistrace) se tak odehrává místně v rámci site (místní sítě) a tyto požadavky nevstupují do sítě WAN. Na odloučených pracovištích, kde není umístěn doménový řadič (v této chvíli nejde o site), bude využíván server DNS mateřské lokality – PSSZ, KSSZ nebo OSSZ.

Na serveru sixx5 je také vytvořena zóna net.cssz.cz, která obsahuje dns jména aktivních prvků.

3.1.1 Klientské stanice v doméně cssz.cz

Stanice mají nastaven jako primární DNS server vždy nejbližší DNS server SIZZ1 v rámci site a sekundární server DNS v ústředí sixx5. Výjimku tvoří ústředí a krajské sídla, kde je možné jako druhé dns použít druhý doménový řadič SIZZ2

3.1.2 Servery v sídle OZZ,KZZ

Servery včetně unxiových, mají nastaven jako primární DNS server vždy nejbližší DNS server SIZZ1 v rámci site a sekundární server DNS v ústředí SIXX5.

3.1.3 Servery v sídle UXX a APP

Servery včetně unixových, mají nastaven jako primární DNS server SIXX5 a sekundární server SIXX6.

3.1.4 Jmenná syntaxe

Pro pojmenování počítačů je používána následující syntaxe:
a+XX+4místné číslo počítače+suffix cssz.cz, přičemž:
XX značí lokalitu, kde je umístěn daný počítač

U serverů je jmenná syntaxe následující:
Si/a+XX+číslo serveru v lokalitě+sufix cssz.cz, přičemž:
Si – toto pojmenování se používá pro doménové controllery
Sa - toto pojmenování je použito pro aplikační servery
XX značí lokalitu, kde je umístěn daný server

Jmennou syntaxi domény net.cssz.cz popisuje samostatný dokument (Standard síťové infrastruktury).

3.2 DNS & Active Directory app.cssz.cz

DNS servery aplikační vrstvy, realizované na doménových řadičích domény app.cssz.cz, spravují mimo samotnou root zónu „.“app.cssz.cz a patřičnou reverzní zónu (obě jako *active directory integrated* replikovány v rámci replikace AD) následující domény:

appv.cssz.cz
db.cssz.cz
ext.cssz.cz

Doména appv.cssz.cz obsahuje jména virtuálních služeb aplikačních serverů dle specifikace jednotlivých služeb (aplikací).

Doména db.cssz.cz obsahuje jména jednotlivých databázových služeb.

Doména ext.cssz.cz obsahuje jména externě poskytovaných služeb (např. SAP).

3.2.1 Jmenná syntaxe

V doméně app.cssz.cz je syntaxe následující:

Servery:
Sa+XX+číslo serveru v lokalitě (např. 001)+sufix app.cssz.cz, přičemž:
Sa - toto pojmenování je použito pro aplikační servery
XX značí lokalitu, kde je umístěn daný server (1X pro KP1, 2X pro KP2)

Každý server může mít vytvořen alias ve formátu jméno alikace + pořadové číslo (nem1.app.cssz.cz)

V doméně appv.cssz.cz jsou jména virtuálních služeb aplikačních serverů tvořena názvem aplikace a sufixem, tedy např. nem.appv.cssz.cz, přičemž testovací prostředí je uvozeno znaky t-, tedy např. t-nem.appv.cssz.cz.

V doméně db.cssz.cz jsou jména jednotlivých služeb, které jsou použity pro přístupy jednotlivých aplikací do DB, čímž v budoucnu bude zajištěna jednoduší migrace DB mezi servery. Jmenná konvence je navržena, aby vyhověla jak DB Oracle, tak DB MS SQL následujícím způsobem:

Jmenná konvence - yxxxxzmn

- y - první znak – specifikace prostředí
  - P - produkční
  - T - testovací
  - D - vývojové
  - I - integrační
  - S - systémové

- xxxx - jméno DB instance nebo schématu – max. délka 4 znaky

  Pozn: V případě, že je název DB kratší než 4 znaky, bude délka názvu doplněna na délku 4 znaků zástupným znakem „X“. Znak bude umisťován na konec jména DB instance.

- z - šestý znak
  - O - Oracle
  - S - MS SQL

- m - sedmý znak - specifikace režimu DB
  - S - StandAlone DB
  - R - vysoká dostupnost řešena prostřednictvím RAC
  - H - vysoká dostupnost řešena prostřednictvím HACMP nebo MS CS
  - Z - záložní DB

- n - pořadové číslo
  - 1 - číslo bude použito pro všechny DB v režimu HACMP, MS CS, a první CE NAME VIP nódu RAC
  - 2 - číslo 2 bude použito pro druhý CE NAME VIP nódu RAC

Např. ukázka specifikace CE NAME záznamů pro RAC – produkční INP:

Nóde 1 RAC	PINPXOR1.db.cssz.cz
Testovací Nóde 2 RAC	TINPXOR2.db.cssz.cz

3.3 DNS & management zóna

DNS server pro management vrstvu je postaven na doménovém řadiči domény cssz.cz v této vrstvě, navíc jsou dále na tento DNS server přenášeny všechny DNS zóny z DNS serverů aplikační vrstvy (appv.cssz.cz, app.cssz.cz, ext.cssz.cz a db.cssz.cz) a zóna net.cssz.cz z DNS serveru sixx5. Slouží jako proxy služba pro transfery zon z různých vrstev sítí.

3.4 DNS & Internet

Pro poštovní smtp relaye, zajišťují překlad internetových adres DNS1-XX DNS-2X v DMZ ČSSZ. Pro proxy službu běžící služba DNS na upstream serverech PX1-XX a PX1_2X. Podle požadavku forwardují a zároveň na určitou dobu ukládají do paměti překlady ze serverů:

- Pro doménu cssz.cz ze serveru: 10.1.140.125
- Pro Internetní domény ze serverů 10.20.1.10, 10.20101.10
- Pro TESTu ze serveru v GovNetu 14.154.254.21
- pro doménu Govbone, MPSV a MFCR ze serveru 192.168.248.20

4. SLUŽBY DHCP

Služba DHCP je instalována v doméně cssz.cz na serverech *Windows Server 2003* konfigurovaných jako doménové řadiče. Protože v každé lokalitě může být provozován vždy pouze jediný server DHCP, není v lokalitách, kde je instalováno více doménových řadičů (KSSZ a Ústředí), DHCP na dalších serverech instalováno. Služba DHCP není instalována ani na žádném ze serverů v centrální site UXX.

V rámci Ústředí je jak je výše uvedeno provozován jeden server s instalovanou službou DHCP, přičemž obsluhuje klienty z různých sítí díky možnosti vytvoření více oborů adres IP (IP scopes) v rámci jednoho serveru (v rámci aktivních prvků je spuštěna služba DHCP Relay Agent).

Každý počítač, na němž je nainstalován operační systém *Windows 2000* nebo *Windows XP*, registruje záznamy typu A a PTR. Tuto činnost zajišťuje služba DHCP, a to i v případech, že pro přidělení IP parametrů není DHCP využíváno. Pokud klientovi vyprší doba propůjčení IP adresy (lease expired), DHCP server zajistí kromě uvolnění IP adresy v definovaném scope i odstranění záznamů typu A a PTR z DNS. Doba platnosti každého dynamicky vytvořeného záznamu je stanovena na 8 dní.

Rezervace IP adres jsou využívány jen ve zcela specifických případech.

4.1 Scope

V rámci organizace ČSSZ jsou definovány scopes pro různé typy zařízení (viz. tabulka č.1) a lokality. V rámci každé lokality je definován právě jeden scope, výjimkou je lokalita Ústředí, kde jsou definovány scopes pro jednotlivá zařízení. Zástupný znak x ve druhém byte adresy IP reprezentuje příslušnou lokalitu. Přehled těchto lokalit s uvedením číslice druhého byte adresy IP je uveden v tabulce č.3..

Tabulka č.1 – Rozsah IP adres pro vybraná zařízení

Rozsah adres IP	Typ zařízení
10.x.1.1 – 10.x.5.254	Desktopy
10.x.6.1 – 10.x.6.254	Servery
10.x.7.1 – 10.x.7.254	Spravované aktivní prvky pro LAN (switch, hub, UPS)
10.x.190.1 – 10.x.190.254	Spravované aktivní prvky pro WAN (směrovač, šifrátor)
10.x.200.1 - 10.x.200.254	Bridge pro připojené OP

Tabulka č.2 – Definované scopes pro lokality

Parametry	Nastavení
Rozsah IP	10.x.1.1 - 10.x.2.254
Subnet Mask	255.255.0.0
Exclusions	x.x.x.x, x.x.x.x, x.x.x.x - x.x.x.x
Rezervace	x.x.x.x - x.x.x.x
Doba pronájmu	8 dní

Tabulka č.3 - Přehled lokalit s uvedením číslice druhého byte adresy IP

Lokalita	Označení site	Druhý byte adresy sítě IP
PSSZ Praha	PXA	42
ÚP Praha1	P1A	78
ÚP Praha2	P2A	80
ÚP Praha3	P3A	81
ÚP Praha4	P4A	82
ÚP Praha5	P5A	83
ÚP Praha6	P6A	84
ÚP Praha7	P7A	85
ÚP Praha9	P9A	87
ÚP Praha10	P0A	79
ÚP Praha21	PAA	114
ÚP Praha22	PBA	115
KSSZ Praha (Středočeský kraj)	KPH	88
OSSZ Benešov	OBN	21
OSSZ Beroun	OBE	22
OSSZ Kladno	OKL	53
OSSZ Kolín	OKO	55
OSSZ Kutná Hora	OKH	57
OSSZ Mělník	OME	62
OSSZ Mladá Boleslav	OMB	64
OSSZ Nymburk	ONB	66
OSSZ Praha-západ	OPZ	89
OSSZ Příbram	OPB	91
OSSZ Rakovník	ORA	93
KSSZ České Budějovice	KCB	31

Lokalita	Označení site	Druhý byte adresy sítě IP
OSSZ Český Krumlov	OCK	32
OSSZ Jindřichův Hradec	OJH	51
OSSZ Písek	OPI	73
OSSZ Prachatice	OPT	77
OSSZ Strakonice	OST	98
OSSZ Tábor	OTA	101
KSSZ Plzeň	KPJ	74
OSSZ Plzeň – město	OPM	75
OSSZ Plzeň – sever	OPS	76
OSSZ Domažlice	ODO	35
OSSZ Klatovy	OKT	54
OSSZ Rokycany	ORO	94
OSSZ Tachov	OTC	102
KSSZ Karlovy Vary	KKV	58
OSSZ Cheb	OCH	28
OSSZ Sokolov	OSO	97
KSSZ Liberec	KLB	59
OSSZ Česká Lípa	OCL	33
OSSZ Jablonec nad Nisou	OJN	48
OSSZ Semily	OSM	96
KSSZ Ústí nad Labem	KUL	106
OSSZ Děčín	ODC	34
OSSZ Chomutov	OCV	29
OSSZ Litoměřice	OLT	60
OSSZ Louny	OLN	61
OSSZ Most	OMO	63
OSSZ Teplice	OTP	103
KSSZ Hradec Králové	KHK	46
OSSZ Jičín	OJC	49
OSSZ Náchod	ONA	65
OSSZ Rychnov nad Kněžnou	ORK	95
OSSZ Trutnov	OTU	105
KSSZ Pardubice	KPA	71
OSSZ Chrudim	OCR	30

Lokalita	Označení site	Druhý byte adresy sítě IP
OSSZ Svitavy	OSY	100
OSSZ Ústí nad Orlicí	OUO	107
KSSZ Jihlava	KJI	50
OSSZ Havlíčkův Brod	OHB	47
OSSZ Pelhřimov	OPE	72
OSSZ Třebíč	OTR	104
OSSZ Žďár nad Sázavou	OZR	111
KSSZ Brno	KBI	26
OSSZ Blansko	OBK	23
OSSZ Břeclav	OBV	24
OSSZ Hodonín	OHO	45
OSSZ Vyškov	OVY	110
OSSZ Znojmo	OZN	113
MSSZ Brno	MBM	25
KSSZ Olomouc	KOC	68
OSSZ Jeseník	OJE	117
OSSZ Prostějov	OPV	92
OSSZ Přerov	OPR	90
OSSZ Šumperk	OSU	99
KSSZ Ostrava	KOS	70
OSSZ Bruntál	OBR	27
OSSZ Frýdek Místek	OFM	44
OSSZ Karviná	OKI	52
OSSZ Nový Jičín	ONJ	67
OSSZ Opava	OOP	69
KSSZ Zlín	KZL	112
OSSZ Kroměříž	OKM	56
OSSZ Uherské Hradiště	OUH	108
OSSZ Vsetín	OVS	109

4.2 Parametry nastavované prostřednictvím DHCP

Prostřednictvím DHCP jsou pro daný scope nastavovány následující vlastnosti:

Tabulka č.4 - Definice scope options v prostředí ČSSZ

DHCP Option	Option **č**íslo	Nastavení
Router	003	10.XX.1.254 (adresa IP default gateway příslušné lokality)
DNS Servers	006	10.XX.6.10, 10.1.140.125 (primární server DNS – DC příslušné lokality a sekundární server DNS sixx5)
DNS Domain Name	015	cssz.cz
WINS/NBNS Servers	044	10.1.140.125, 10.1.140.126 (WINS servery sixx5 a sixx6)
WINS/NBT Node Type	046	0x8 (h-node, nejprve WINS poté broadcast)
Boot Server Host Name	066	*servername*.cssz.cz (název serveru RIS v příslušné lokalitě)
Bootfile name	067	OSChooser\i386\startrom.com

5. SLUŽBY NTP

Služba NTP zajišťuje jednotné nastavení času v celém informačním systém ČSSZ. Zdrojem času jsou servery v Internetu tik.cesnet.cz na které se synchronizuje server v DMZ (ntp1.cssz.cz). Z tohoto serveru jsou synchronizovány servery v DMZ, centrální doménové řadiče (ntp2.cssz.cz) a centrální LAN prvky řady Cisco 6500.. Další distribuce času je zajištěna nativní službou systému v rámci doménové infrastruktury mezi jednotlivými řadiči. Z doménových serverů získávají informace o času automaticky stanice a servery, které jsou zařazeny do domény. Ostatní servery (mimo doménu) na územních organizačních jednotkách se synchronují protokolem NTP také na doménový řadič lokality (např. Solaris pomocí CRONu: 30 05 * * * /usr/sbin/ntpdate -s 10.zz.6.10).

Doménové servery domény app.cssz.cz se synchronizují s doménovým řadičem umístěným v management vrstvě, který poskytuje služby NTP i pro ostatní servery management vrstvy jako ntp3.cssz.cz.