System i

Síťové technologie
E-mail

verze 6 vydání 1

System i

Síťové technologie
E-mail

verze 6 vydání 1

Poznámka

Před použitím této příručky a produktů, jichž se týká, si přečtěte informace v části “Poznámky”, na stránce 51.

Toto vydání se vztahuje k verzi 6, vydání 1, modifikaci 0 operačního systému IBM i5/OS (číslo produktu 5761-SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno něco jiného. Tuto verzi nelze provozovat na všech modelech RISC (reduced instruction set computer) ani na modelech CISC.

Obsah

E-mail

Tyto informace můžete využít při plánování, konfigurování, používání, správě a odstraňování problémů s e-mailem ve vašem systému.

Tyto pokyny předpokládají, že jste již se systémem i5/OS pracovali, a máte praktické zkušenosti s TCP/IP, SMTP (Simple Mail Transfer Protocol) a s koncepcemi e-mailu.

Co je nového ve verzi V6R1

Zde se seznámíte s novými nebo zásadně změněnými informacemi v kolekci témat E-mail ve verzi V6R1.

Podpora SMTP S/MIME

Protokol (S/MIME) (secure/Multipurpose Internet Mail Extensions) je možné použít k ověření odesílatelů e-mailu, pokud je v doručeném SMTP (Simple Mail Transfer Protocol) více transakcí. Pomocí tohoto protokolu je možné e-mailový dokument podepsat nebo zašifrovat. Podporu protokolu S/MIME poskytuje nové rozhraní QtmsCreateSendEmail API.

V následujících tématech najdete definici protokolu S/MIME a popis konfiguračních kroků nutných k použití tohoto nového rozhraní API:

- “Koncepce elektronické pošty” na stránce 2
- “Scénář: Konfigurace rozhraní QtmsCreateSendEmail API pro používání S/MIME” na stránce 6

Autentizace SMTP a podpora SSL/TLS

Pomocí autentizace SMTP nyní můžete vysledovat původce e-mailu. Server SMTP operačního systému i5/OS také podporuje relace, které jsou chráněné pomocí protokolu SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security).

- “Řízení přístupu pomocí protokolu SMTP” na stránce 10
- “Sledování odesílatele e-mailu” na stránce 24

Server POP podporuje relace SSL/TLS

Server POP (Post Office Protocol) operačního systému i5/OS nyní podporuje relace SSL/TLS. Server může šifrovat ID uživatele a hesla.

- “Nastavení e-mailových klientů POP” na stránce 28

Jak zjistíte, které informace jsou nové nebo změněné

Abyste mohli snadno rozpoznat, kde byly provedeny technické změny, je v těchto informacích použito následující označení:

- Obrázek » k označení místa, kde začínají nové nebo změněné informace.
- Obrázek « k označení místa, kde nové nebo změněné informace končí.

V souborech ve formátu PDF se u nových nebo změněných informací můžete setkat na levém okraji s revizními značkami (|).

Další informace o tom, co je v tomto vydání nové nebo co se změnilo, naleznete v dokumentu Sdělení uživatelům.

Soubor ve formátu PDF pro publikaci E-mail

Soubor s těmito informacemi ve formátu PDF si můžete zobrazit a vytisknout.

Chcete-li zobrazit nebo stáhnout tento dokument ve formátu PDF, klepněte na tento odkaz: E-mail (cca 692 kB).

Jak uložit soubor ve formátu PDF

Pokud chcete uložit soubor ve formátu PDF na pracovní stanici za účelem prohlížení nebo tisku, postupujte takto:

1. Klepněte pravým tlačítkem myši na odkaz na PDF ve vašem prohlížeči.
2. Klepněte na volbu pro uložení PDF do místního počítače.
3. Přejděte do adresáře, do kterého chcete PDF uložit.
4. Klepněte na tlačítko **Uložit**.

Stažení programu Adobe Reader

K prohlížení nebo tisku souborů ve formátu PDF potřebujete mít v systému nainstalován produkt Adobe Reader. Jeho bezplatnou kopii si můžete stáhnout z webu společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Související odkazy

"Informace související s e-mailem" na stránce 49

Produktové manuály, publikace IBM Redbooks, webové stránky a další informace v kolekcích témat aplikace Informační centrum, které se vztahují ke sbírce témat E-mail. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Koncepce elektronické pošty

V dnešní době jste závislí na elektronické poště jako na základním pracovním nástroji. Operační systém i5/OS používá protokoly, jako například SMTP (Simple Message Transfer Protocol) a POP (Post Office Protocol), aby byly vaše e-maily přijímány a odesílány po síti hladce a efektivně.

Distribuční metody

Tyto dodatečné e-mailové koncepce pojednávají o dalších e-mailových distribučních metodách:

- MIME (Multipurpose Internet Mail Extensions)

  MIME je standardizovaná metoda, která slouží k uspořádání různých formátů souborů. Protokol SMTP je omezen na 7bitový text ASCII s maximální délkou řádky 1000 znaků. MIME byl vyvinut pro podporu pokročilejších typů souborů, jako je například RTF, obrázky a audio nebo video soubory. MIME kóduje soubory binárních typů dat tak, aby data vypadala jako jednoduchá data SMTP, a používá přitom záhlaví k odlišení různých typů souborů v rámci zprávy ještě před jejím odesláním pomocí protokolu SMTP. Poštovní klient obdrží zprávu a dekóduje ji na původní typy souborů pomocí interpretace záhlaví MIME při čtení souboru.
- S/MIME

  Secure/MIME je zabezpečená verze protokolu MIME, která umožňuje uživatelům odeslat šifrované a elektronicky podepsané e-mailové zprávy i v případě, že uživatelé mají různé e-mailové programy.
- Framework AnyMail/400

  Veškerá příchozí pošta ze serveru SMTP pro lokální uživatele (uživatele s poštovními účty na tomto systému) je zpracována frameworkem AnyMail/400. Tento framework představuje strukturu distribuce elektronické pošty. Framework poštovního serveru volá programy výstupního bodu nebo programy typu snap-in, aby mohl pracovat s určitými typy elektronické pošty.
- SNADS (Systems Network Architecture Distribution Services)

  SNADS (System Network Architecture Distribution Services) je asynchronní distribuční služba IBM, která definuje řadu pravidel pro přijímání, směrování a odesílání elektronické pošty v síti systémů. V tomto tématu služba SNADS

odkazuje na uživatelský profil, ve kterém je **Preferovaná adresa** nastavena na **ID uživatele/adresa**. Preferovaný typ adresy říká frameworku poštovního serveru, jaké pole má použít pro adresu v systémovém distribučním adresáři.

Související pojmy

"Odeslání a přijetí e-mailu" na stránce 28
Váš systém je poštovní server a jsou na něm zapsáni e-mailoví uživatelé (uživatelé SNADS, POP nebo Lotus). Pomocí klienta POP nebo SNADS mohou tito uživatelé odesílat, přijímat nebo číst e-mail.

Související úlohy

"Pozastavení front služeb SNADS" na stránce 12
Distribuční fronty služeb SNADS (Systems Network Architecture Distribution Services) používané aplikací SMTP k distribuci pošty lze pozastavit. Tím získáte další ochranu omezující distribuci pošty.

Protokol SMTP v operačním systému i5/OS

Protokol SMTP (Simple Mail Transfer Protocol) je protokol, který umožňuje operačnímu systému odesílat a přijímat e-mail.

Protokol SMTP je v podstatě průběžné doručování e-mailu z jednoho poštovního serveru na druhý. Mezi odesílatelem SMTP (klientem) a cílovým příjemcem SMTP (serverem) existuje přímé spojení. Klient SMTP uchovává e-mailové zprávy u odesílatele, dokud je úspěšně nepřenese a nezkopíruje pro příjemce SMTP (server).

Protokol SMTP v tomto operačním systému podporuje distribuci poznámek, zpráv a textových dokumentů ASCII. Protokol SMTP podporuje i jiné formáty, než prostý text, a to pomocí protokolu MIME (Multipurpose Internet Mail Extensions). Protokol MIME je internetovým standardem pro odesílání e-mailu se záhlavími, která přijímajícímu klientovi popisují obsah poštovních zpráv. Tyto zprávy mohou obsahovat video, audio i binární části.

Doručování e-mailu pomocí protokolu SMTP

Aby e-mail dorazil na místo určení, musí být protokol SMTP schopen doručit tuto poštu správnému hostiteli s příslušným ID uživatele. Předpokládejme, že je pošta odeslána na adresu bobsmith@mycompany.com.

Protokol SMTP nejdříve zkontroluje, zda je e-mailový adresát (bobsmith) uživatelem na lokálním serveru. Jestliže protokol SMTP zjistí, že není, předá e-mail dalšímu hostitelskému serveru. Další hostitel může, ale také nemusí, být konečným hostitelem. Protokol SMTP určí jméno hostitele z informace o adresování, která se nachází v protokolu SMTP.

Protokol SMTP potom určí adresu hostitele buď pomocí serveru DNS (Domain Name Server), nebo pomocí lokální hostitelské tabulky. Hostitelské jméno používají lidé jako část názvu e-mailového účtu (mycompany.com). Adresu IP používá protokol SMTP k nalezení správného poštovního serveru, na který odešle poštu (192.1.1.10).

1. Server SMTP při vyhledávání adres hostitelského jména v lokální hostitelské tabulce ignoruje adresy IPv6.
2. Pokud některé nakonfigurované servery DNS mají adresy IPv6, potom musí všechny nakonfigurované servery DNS podporovat rekurzivní vyhledávání, aby mohly být zjištěny e-mailové domény, k nimž tyto nakonfigurované servery nemají oprávnění.

Tato témata se týkají DNS a SMTP:

- Nastavení domény DNS (Domain Name System)
- Pošta a záznamy MX (Mail Exchanger)

V případě příchozího e-mailu server SMTP nejdříve převede cílové hostitelské jméno na adresu IP (Internet Protocol). Díky funkci alias může mít server několik hostitelských jmen. Server SMTP proto používá rozhraní typu socket, aby určil, zda je IP adresa jednou z adres, které jsou využívány rozhraními lokálního hostitele.

Související pojmy

DNS

Záznamy Mail and Mail Exchanger

Související úlohy

Nastavení domény DNS (Domain Name System)

“Konfigurace e-mailu” na stránce 13
Chcete-li nastavit e-mail na vašem systému, musíte nakonfigurovat TCP/IP, nastavit server SMTP a POP server a spustit e-mailové servery.

Protokol POP v operačním systému i5/OS

Server POP (Post Office Protocol) je e-mailové rozhraní implementované v operačním systému i5/OS. Jedná se o Post Office Protocol verze 3.

Server POP poskytuje v tomto operačním systému e-mailové schránky, které mohou klienti používat pro příjem pošty. Každý poštovní klient, který podporuje protokol POP3, jako například Netscape Mail, Outlook Express nebo Eudora, může používat tento server. Klienty lze provozovat na libovolné platformě, například Windows, Linux, AIX nebo Macintosh.

Server POP slouží jako dočasné úložiště e-mailu do doby, dokud ji poštovní klient nenačte. Když se poštovní klient připojí k serveru, dotáže se na obsah své poštovní schránky, aby zjistil zda má nějakou poštu k načtení. Pokud zde taková pošta je, načte ji po jednotlivých zprávách. Po načtení zprávy klient přikáže serveru, aby tuto zprávu označil k vymazání, jakmile skončí klientská relace. Klient načte všechny zprávy v poštovní schránce a potom vydá serveru příkaz k vymazání všech zpráv, které jsou označeny pro výmaz, a k ukončení spojení s klientem.

E-mailoví klienti POP používají při komunikaci se serverem POP příkazy *verb*. Příkazy verb podporované serverem POP pro tento operační systém jsou popsány v tématu Protokol POP (Post Office Protocol).

Související úlohy

“Přistupování k e-mailovým serverům prostřednictvím produktu System i Navigator” na stránce 13
Produkt System i Navigator můžete použít ke konfigurování a správě e-mailových serverů s protokoly SMTP (Simple Mail Transfer Protocol) a POP (Post Office Protocol).

“Konfigurování serverů SMTP a POP pro e-mail” na stránce 14
Chcete-li používat e-mail, musíte nakonfigurovat servery SMTP a POP ve vašem systému.

Související odkazy

“Protokol POP (Post Office Protocol)” na stránce 44
Poštovní rozhraní POP (Post Office Protocol) verze 3 je definováno v dokumentech RFC (Request for Comments) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism) a RFC 2595 (Using TLS with IMAP, POP3, and ACAP). Dokumenty RFC slouží k definování vyvíjejících se internetových standardů.

Související informace

RFC Index

Scénář: E-mail

Tento scénář ukazuje proces zpracování pošty mezi lokálními uživateli a způsob konfigurování rozhraní QtmsCreateSendEmail API pro použití protokolu S/MIME.

Scénář: Lokální odeslání a přijetí e-mailu

Tento příklad ukazuje proces zpracování pošty mezi lokálními uživateli.

Situace

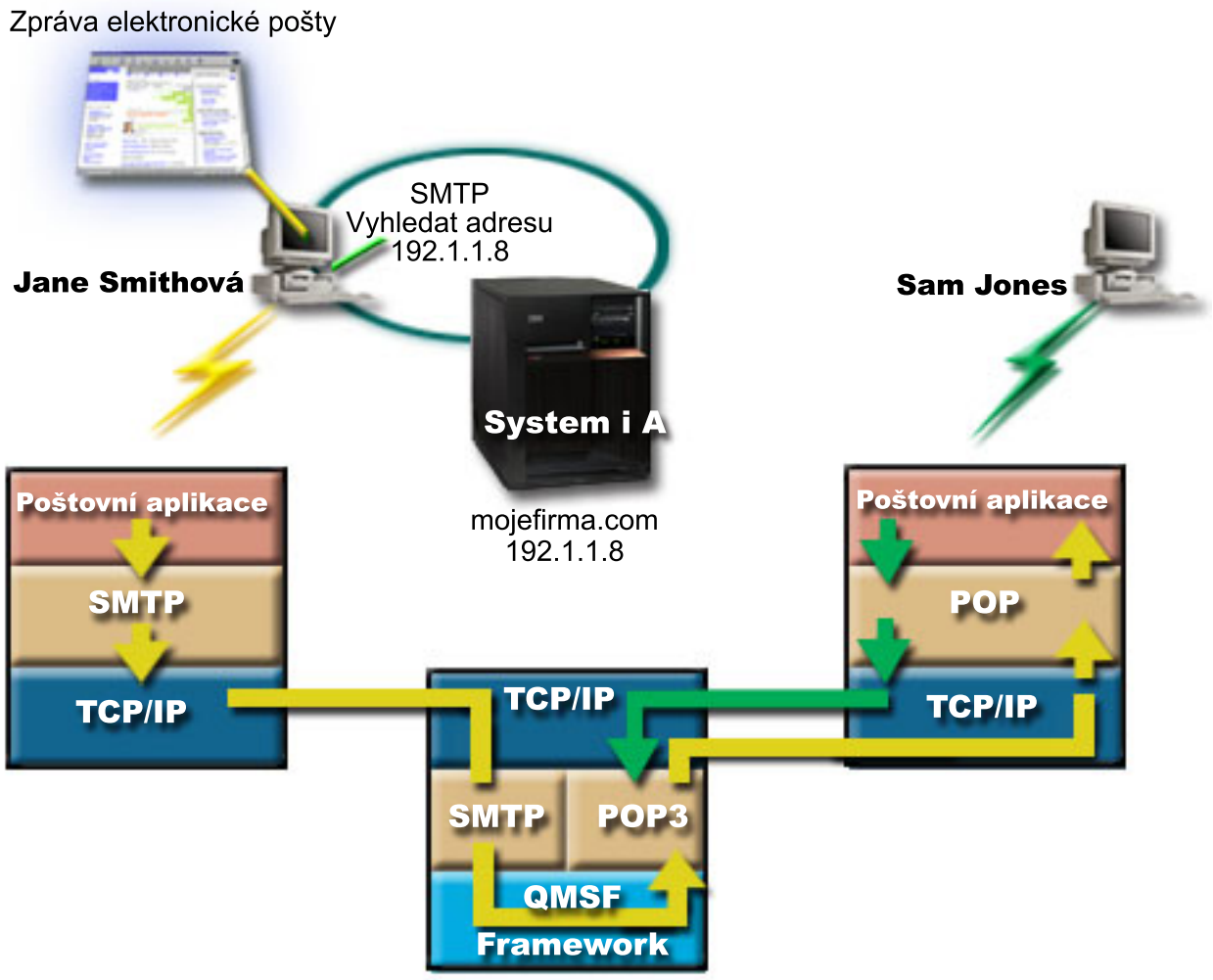
Jane Smithová, ředitelka personálního oddělení, potřebuje odeslat zprávu Samovi Jonesovi z právního oddělení. Oba pracují v ústředí firmy MyCompany. Sledujte tento proces a poznáte, jakým způsobem systém zpracovává e-mail.

Cílem tohoto příkladu je:

- Ukázat, jak spolu poštovní klienti a servery vzájemně souvisejí a jak je zpracovávána zpráva.
- Jak použít server SMTP k odeslání pošty.
- Jak tuto poštu doručit uživateli POP.

Podrobnosti

Jane používá poštovního klienta Netscape. Napíše zprávu a odešle ji na adresu SamJones@mycompany.com. Následující obrázek znázorňuje cestu, kterou pošta projde sítí.



Obrázek 1. Ukázka konfigurace sítě

Následující text popisuje každou fázi cesty, kterou projde poštovní zpráva v rámci sítě.

Fáze 1: Z klienta SMTP na server SMTP

Klient SMTP na PC, jenž používá Jane, použije konfigurační data, která byla zadána pro odchozí server a identitu. Pole identity se použije pro adresu odesilatele **Od:**. Odchozí server je hostitelem, s kterým PC klient SMTP naváže spojení. Jelikož je tato adresa zadána jako doména, klient SMTP požádá DNS o IP adresu serveru SMTP a zjistí, že adresa je 192.1.1.8.

Klient SMTP se nyní spojí se serverem SMTP na portu SMTP (port 25 na 192.1.1.8). Dialog používaný mezi klientem a serverem je protokol SMTP. Server SMTP potvrdí přijetí pošty a zpráva je pomocí protokolu TCP/IP přenesena z klienta na server.

Fáze 2: Server SMTP doručí zprávu na server POP

Server SMTP ověří doménu příjemce, a zjistí, zda je lokální. Vzhledem k tomu, že je doména příjemce lokální, zapíše se pošta do integrovaného systému souborů a rozhraní QMSF Framework Create Message API uloží informaci o zprávě do fronty QMSF. Framework QMSF umožní distribuci e-mailu, volání programů výstupního bodu a programů typu snap-in pro zpracování určitých typů pošty. Z informace o zprávě určí, že Samova adresa je ve formátu SMTP, takže framework zavolá program výstupního bodu SMTP Address Resolution. Tento program opět ověří, zda je zpráva lokální. Protože je lokální, použije k vyhledání adresy SMTP příjemce distribuční adresář (data jsou zadána pomocí příkazu WRKDIRE). Program výstupního bodu najde Samovu adresu a zjistí, že úroveň e-mailových služeb je paměť systémových zpráv v adresářovém záznamu tohoto uživatele. Proto jej rozpozná jako účet POP. Program SMTP Address Resolution pak přidá informaci ze Samova profilu do informace o zprávě. Označí tuto informaci jako POP local delivery (lokální doručení POP). Framework QMSF potom zavolá program výstupního bodu POP Local Delivery, který najde informace o profilu a jméno integrovaného systému souborů a doručí poštu do Samovy poštovní schránky.

Fáze 3: Klient POP načte zprávu pro Sama Jonese ze serveru POP

O něco později se Sam rozhodne, že si pomocí e-mailového klienta (Netscape) zkontroluje svou poštu ve schránce. Klient POP na jeho PC je nakonfigurován tak, aby kontroloval přístup k serveru POP na mycompany.com pro uživatelské jméno SamJones a heslo (******). Jméno domény se opět změní na IP adresu (pomocí DNS). Klient POP se spojí se serverem POP pomocí portu POP a protokolu POP3. Server POP v operačním systému zkontroluje, zda jméno a heslo uživatele poštovní schránky odpovídají profilu a heslu uživatele operačního systému i5/OS. Jakmile je ověření ukončeno, použije se jméno profilu k nalezení Samovy poštovní schránky. Klient POP načte zprávu a odešle zpět na server POP požadavek na vymazání pošty z poštovní schránky POP. Zpráva se pak zobrazí na klientovi Netscape a Sam si ji může přečíst.

Související pojmy

"Plánování e-mailu" na stránce 9
Před nastavením e-mailu byste měli mít základní představu o tom, jakým způsobem jej budete na systému používat.

Související odkazy

"SMTP (Simple Mail Transfer Protocol)" na stránce 43
SMTP (Simple Mail Transfer Protocol) je protokol protokolu TCP/IP používaný k odesílání a přijímání elektronické pošty. Obvykle se spolu s protokolem POP3 nebo IMAP (Internet Message Access Protocol) používá k uložení zpráv do schránky elektronické pošty na serveru a k jejich pravidelnému stahování ze serveru pro uživatele.

"Protokol POP (Post Office Protocol)" na stránce 44
Poštovní rozhraní POP (Post Office Protocol) verze 3 je definováno v dokumentech RFC (Request for Comments) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism) a RFC 2595 (Using TLS with IMAP, POP3, and ACAP). Dokumenty RFC slouží k definování vyvíjejících se internetových standardů.

Scénář: Konfigurace rozhraní QtmsCreateSendEmail API pro používání S/MIME

Tento scénář demonstruje, jak můžete nakonfigurovat rozhraní QtmsCreateSendEmail API pro používání secure/MIME (S/MIME).

Situace

Uživatel John Smith, jehož ID uživatele je jsmith, chce nakonfigurovat rozhraní QtmsCreateSendEmail API pro používání S/MIME. S/MIME je zabezpečenější způsob pro programové odesílání e-mailů, než je použití rozhraní QtmmSendMail API.

Podrobnosti

Chce-li John odeslat podepsané a šifrované e-maily, potřebuje mít na svém systému, kde je spuštěn i5/OS V6R1, nainstalované následující volby:

- i5/OS PASE (5761-SS1 volba 33)
- Digital Certificate Manager (5761-SS1 volba 34)
- OpenSSL (5733-SC1 volba 1)

Vytvoření úložiště uživatelských certifikátů

Použití S/MIME vyžaduje úložiště uživatelských certifikátů, které se nazývá user certificate store. V operačním systému platí pro uživatelské certifikáty pojmenovávací konvence *userid*.usrcrt. Certifikáty jsou v adresáři /qibm/userdata/icss/cert/download/client.

John musí vytvořit úložiště uživatelských certifikátů pro svůj vlastní uživatelský profil, pod nímž je spuštěna úloha pro vytváření a odesílání e-mailových zpráv. Ke spravování úložiště uživatelských certifikátů může použít DCM (Digital Certificate Manager).

Jestliže chcete vytvořit úložiště uživatelských certifikátů, postupujte následujícím způsobem:

1. Vytvořte podadresář použitím jména profilu uživatele:

   ```
   cd  /qibm/userdata/icss/cert/download/client
   mkdir  jsmith
   ```

2. Pomocí webového prohlížeče přejděte na stránku Úlohy System i na vašem systému na http://*jméno_systému*: 2001.
3. Chcete-li získat přístup k uživatelskému rozhraní DCM, vyberte ze seznamu produktů **Správce digitálních certifikátů** na stránce Úlohy System i. V levém podokně klepněte na **Vytvořit nové úložiště certifikátů**.
4. Na stránce Vytvořit nové úložiště certifikátů, vyberte **Úložiště certifikátů jiného systému** a klepněte na **Pokračovat**.
5. Na stránce Vytvořit certifikát v novém úložišti certifikátů vyberte **Ne - nevytvořit certifikát v úložišti certifikátů**.
6. Na stránce Jméno úložiště certifikátů a heslo vyplňte jméno cesty úložiště certifikátů a heslo. Nastavte cestu úložiště certifikátů tak, aby zahrnovala ID uživatele. Například John nastaví cestu ke svému úložišti na /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.

Export uživatelského certifikátu odesílatele do System i

Johnův webový prohlížeč je IE 6 (Internet Explorer verze 6). Uživatelský certifikát odesílatele uděluje (Certificate Authority) a nainstaluje se na IE 6.

Chce-li exportovat uživatelský certifikát odesílatele na platformu System i, provede John následující kroky:

1. V okně IE vyberte **Nástroje → Možnosti sítě Internet**.
2. Na záložce **Obsah** klepněte na **Certifikáty**.
3. Na kartě **Osobní** vyberte certifikát odesílatele a klepněte na **Exportovat...**.
4. Na stránce Vítá vás Průvodce exportem certifikátu klepněte na **Další**.
5. Na stránce Exportovat soukromý klíč vyberte **Ano, exportovat soukromý klíč** a klepněte na **Další**.
6. Na stránce Formát souboru pro export vyberte **Povolit silnou ochranu (vyžaduje IE 5.0, NT 4.0 SP4 nebo vyšší)** pod **Formát Personal Information Exchange - PKCS č. 12 (.PFX)**.
7. Na stránce Heslo zadejte heslo pro certifikát.
8. Na stránce Soubor pro export zadejte jméno souboru, který chcete exportovat, například C:\temp\jsmithcert.pfx a klepněte na **Další**.
9. Na stránce Dokončení Průvodce exportem certifikátu klepněte na **Dokončit**.

10. Odešlete uživatelský certifikát odesílatele jsmithcert.pfx použitím FTP v ASCII režimu přenosu na platformu System i. V tomto příkladu se předpokládá, že je soubor odeslaný do adresáře integrovaného systému souborů /home/jsmith System i. Detailní informace o tom, jak importovat tento certifikát, najdete v tématu “Import certifikátu odesílatele do System i”.

Export uživatelských certifikátů příjemce do System i

Chce-li John exportovat příjemcův certifikát odesílatele na platformu System i, provede následující kroky:

1. V okně IE vyberte **Nástroje → Možnosti sítě Internet**.
2. Klepněte na záložku **Obsah** na stránce Možnosti sítě Internet a pak klepněte na **Certifikáty...**.
3. Na kartě **Osobní** na stránce Internetové volby vyberte certifikát a klepněte na **Exportovat...**.

   Pokud existuje více než jeden certifikát, je třeba opakovat kroky 3 v 7 pro všechny certifikáty.
4. Na stránce Vítá vás Průvodce exportem certifikátu klepněte na **Další**.
5. Na stránce Formát souboru pro export vyberte **Binární X.509, kódování DER (.CER)**.
6. Na stránce Soubor pro export, zadejte jméno souboru, který chcete exportovat, například C:\temp\receiveruser.cer a klepněte na **Další**.
7. Na stránce Dokončení Průvodce exportem certifikátu klepněte na **Dokončit**.
8. Odešlete uživatelský certifikát příjemce receiver.cet použitím FTP v režimu ASCII na platformu System i. V tomto příkladu se předpokládá, že je soubor odeslaný do adresáře integrovaného systému souborů /home/jsmith System i. Detailní informace o tom, jak importovat certifikát příjemce, najdete v tématu “Import certifikátu příjemce do System i”.
9. Opakujte všechny předchozí kroky pro každého příjemce, který je používán v S/MIME.

Import certifikátu odesílatele do System i

John následně potřebuje importovat svůj uživatelský certifikát a soukromý klíč do úložiště uživatelských certifikátů pomocí DCM. Heslo pro importovaný certifikát musí být shodné s heslem úložiště klíčů. Také potřebuje importovat všechny certifikáty uživatelů, kterým chce odesílat e-maily.

1. Pomocí webového prohlížeče přejděte na stránku Úlohy System i na vašem systému na http://*jméno_systému*: 2001.
2. Chcete-li získat přístup k uživatelskému rozhraní DCM, vyberte ze seznamu produktů **Správce digitálních certifikátů** na stránce Úlohy System i.
3. Na stránce Výběr úložiště certifikátů, vyberte **Úložiště certifikátů jiného systému** a klepněte na **Pokračovat**.
4. Na stránce Jméno úložiště certifikátů a heslo zadejte jméno souboru včetně cesty úložiště certifikátů a heslo a klepněte na **Pokračovat**. V případě Johna je jméno souboru /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.
5. Rozbalte **Správa certifikátů → Importovat certifikát**. Vyberte **Server nebo klient** pro import certifikátu odesílatele. Klepněte na **Pokračovat**.
6. Na stránce Import serverového nebo klientského certifikátu zadejte adresář systému integrovaných souborů a jméno souboru certifikátu odesílatele a klepněte na **Pokračovat**. V “Export uživatelského certifikátu odesílatele do System i” na stránce 7 je adresář a jméno souboru /home/jsmith/ jsmithcert.pfx.
7. Zadejte popisek certifikátu, kterým je e-mailová adresa odesílatele malými písmeny. Klepněte na **Pokračovat**.
8. Klepněte na **OK**.

Import certifikátu příjemce do System i

Chcete-li importovat certifikát příjemce do platformy System i, postupujte následujícím způsobem:

1. Pomocí webového prohlížeče přejděte na stránku Úlohy System i na vašem systému na http://*jméno_systému*: 2001.
2. Chcete-li získat přístup k uživatelskému rozhraní DCM, vyberte ze seznamu produktů **Správce digitálních certifikátů** na stránce Úlohy System i.
3. Na stránce Výběr úložiště certifikátů, vyberte **Úložiště certifikátů jiného systému** a klepněte na **Pokračovat**.

4. Na stránce Jméno úložiště certifikátů a heslo zadejte jméno souboru včetně cesty úložiště certifikátů a heslo a klepněte na **Pokračovat**. V případě Johna je jméno souboru /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.
5. Rozbalte **Správa certifikátů → Importovat certifikát**. Vyberte **Certifikační autoritu (CA)** pro import certifikátu příjemce. Klepněte na **Pokračovat**.
6. Na stránce Import certifikátu certifikační autority (CA), zadejte adresář systému integrovaných souborů a jméno souboru certifikátu příjemce a klepněte na **Pokračovat**. V “Export uživatelských certifikátů příjemce do System i” na stránce 8 je adresář systému integrovaných souborů a soubor pro příjemce /home/jsmith/receiveruser.cer.
7. Zadejte popisek certifikátu CA, kterým je e-mailová adresa odesílatele malými písmeny. Klepněte na **Pokračovat**.
8. Opakujte všechny předchozí kroky pro každý certifikát příjemce, který potřebuje odesílatel používat.

Související pojmy

DCM (Digital Certificate Manager)

Související odkazy

Create and Send MIME E-mail (QtmsCreateSendEmail) API

Plánování e-mailu

Před nastavením e-mailu byste měli mít základní představu o tom, jakým způsobem jej budete na systému používat.

Před nastavením elektronické pošty odpovězte na následující otázky:

1. Jak budou vypadat mé adresy elektronické pošty?
2. Jaká je IP adresa mého serveru DNS (Domain Name Server)?
3. Mám ochrannou bariéru? Je-li odpověď ano, jaká je její IP adresa?
4. Mám poštovní server proxy, směrovač pošty nebo mail relay? Je-li odpověď ano, jaká je její IP adresa?
5. Budu používat databázi Domino?
6. Budu pro příjem pošty používat server i5/OS POP?

Pokud budete chtít, najdete základní informace o tom, jak e-mail funguje ve scénáři pro e-mail.

Budete-li používat server Domino a server SMTP i5/OS, přečtěte si téma Provozování serveru Domino a SMTP na stejném systému. Další informace o serveru Domino, najdete v tématu Domino nebo Lotus Domino na webových stránkách i5/OS.

Pokud neplánujete používat servery s protokoly SMTP nebo POP, zablokujte je, abyste si byli jisti, že tyto servery nebudou použity bez vašeho vědomí.

Související pojmy

“Scénář: Lokální odeslání a přijetí e-mailu” na stránce 4
Tento příklad ukazuje proces zpracování pošty mezi lokálními uživateli.

Domino

Související úlohy

“Konfigurace e-mailu” na stránce 13
Chcete-li nastavit e-mail na vašem systému, musíte nakonfigurovat TCP/IP, nastavit server SMTP a POP server a spustit e-mailové servery.

“Server Domino a SMTP na stejném serveru” na stránce 35
Pokud v témže systému spouštíte servery Domino a SMTP (Simple Mail Transfer Protocol), doporučujeme nakonfigurovat je tak, aby se každý zvlášť vázal na specifickou adresu IP.

Související informace

Lotus Domino for i5/OS

Řízení přístupu k e-mailu

Měli byste řídit, kdo přistupuje k systému prostřednictvím e-mailu. Tím ochráníte svá data před svévolnými útoky.

Tento oddíl poskytuje tipy na ochranu e-mailových serverů před zahlcením nevyžádanou poštou.

Související pojmy

Příklad nezávislých fondů disků

"Určování problémů týkajících se e-mailu" na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Související úlohy

"Omezení předávání zpráv" na stránce 25
Chcete-li lidem zabránit, aby používali váš e-mailový server pro spam nebo pro odesílání velkého množství hromadných e-mailů, můžete použít funkci pro omezení předávání k tomu, abyste určili, kdo může používat váš systém pro předávání zpráv. Avšak nemůžete ověřit váš e-mail, pokud omezíte předávání zpráv.

"Zákaz připojení" na stránce 27
Chcete-li zabezpečit systém, můžete zabránit připojení uživatelů, kteří by mohli zneužít váš e-mailový server.

Související informace

AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet

Řízení přístupu pomocí protokolu SMTP

Chcete-li zabránit tomu, aby byl systém vystaven útokům nevyžádanou nebo nebezpečnou poštou (spam), měli byste řídit přístup pomocí protokolu SMTP (Simple Mail Transfer Protocol).

Pokud chcete, aby měli klienti SMTP přístup k systému, měli byste system chránit před útoky pomocí těchto opatření:

- Pokud je to možné, vyvarujte se používání vstupů *ANY *ANY v systémovém distribučním adresáři. Když váš systém nemá žádné vstupy *ANY *ANY, je mnohem těžší zneužít SMTP k zahlcení systému nebo k přetížení sítě. K zahlcení dojde tehdy, když je vnější paměť zaplněna nežádoucí elektronickou poštou, která je směrována přes váš systém na jiný systém.
- Nastavte pro ASP přiměřené mezní hodnoty, abyste uživatelům zabránili v zaplavení vašeho systému nežádoucími objekty. Zobrazit a nastavit prahové hodnoty pro ASP můžete buď pomocí SST (system service tools) nebo DST (dedicated service tools).
- Nastavte maximální počet předspuštěných úloh, které budou vytvořeny při provádění příkazu CHGPJE. Tím omezíte počet úloh vytvořených během útoku typu odmítnutí služby. Předvolená hodnota pro maximální prahovou hodnotu je 256.
- Omezením přenosu a připojení zabraňte vnějším uživatelům v použití vašeho připojení k odesílání nevyžádané pošty (spamu).
- V systémech, na kterých je provozován i5/OS V6R1, můžete zabránit doručení nevyžádané pošty (spamu) tak, že budete vyžadovat ověření při odesílání e-mailu. Pokud vzdálený server vyžaduje ověření, můžete nastavit ověření na vašem lokálním serveru.

Související odkazy

Příkaz CHGSMTPA (Změna atributů SMTP)

Řízení přístupu pomocí protokolu POP

Chcete-li zabezpečit systém, musíte řídit přístup prostřednictvím protokolu POP.

Chcete-li zabezpečit POP datové toky včetně ID uživatelů a hesel, můžete určit zda POP server používá šifrování. Šifrování je poskytováno v rámci SSL (Secure Sockets Layer) nebo TSL (Transport Layer Security). Chcete-li označit, zda jsou zabezpečené POP relace podporovány, nastavte hodnotu parametru ALWSSL CL příkazu CHGPOPA (Změna atributů POP serveru).

Pokud chcete, aby klienti POP měli přístup k vašemu systému, měli byste zvážit tyto otázky týkající se zabezpečení:

| • Poštovní POP server umožňuje ověřit klienty, kteří se snaží získat přístup ke svým schránkám elektronické pošty.
| Klient odesílá na server ID uživatele a heslo.

  Poštovní POP server ověřuje ID uživatele a heslo porovnáním s uživatelským profilem systému i5/OS a heslem pro tohoto uživatele. Protože nemáte kontrolu nad tím, jak je ID uživatele a heslo uloženo v klientovi POP, budete chtít možná vytvořit zvláštní uživatelský profil, který by měl v systému velmi omezená oprávnění. Abyste zabránili zneužití uživatelského profilu při interaktivní relaci, můžete v uživatelském profilu nastavit tyto hodnoty:
  Nastavte počáteční menu (INLMNU) na *SIGNOFF.
  Nastavte počáteční program (INLPGM) na *NONE.
  Nastavte omezení schopností (LMTCPB) na *YES.

- Abyste zabránili svévolnému zahlcení systému nežádoucími objekty, ujistěte se, že jste pro ASP nastavili odpovídající prahové hodnoty. Prahová hodnota ASP brání zastavení systému kvůli tomu, že operační systém nemá dostatek pracovní paměti. Zobrazit a nastavit prahové hodnoty pro ASP můžete buď pomocí SST (system service tools), nebo DST (dedicated service tools).
- Kromě toho, že musíte zajistit, aby prahová hodnota ASP zabránila zahlcení systému, musíte také zabezpečit, aby měl systém dostatek paměti pro řádné ukládání a odesílání pošty. Nemůže-li váš poštovní server doručit poštu kvůli tomu, že nemá odpovídající paměť pro přechodně uloženou poštu, představuje to pro uživatele problém integrity. Když je využití systémové paměti vysoké, přestane pošta běžet.

  Paměťový prostor obvykle nepředstavuje závažnější problém. Když klient obdrží elektronickou poštu, poštovní server odstraní poštu ze systému.

Související pojmy

"Určování problémů týkajících se e-mailu" na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Zabránění v přístupu k e-mailu

V závislosti na tom, jak systém používáte, můžete uživatelům zabránit v přístupu k elektronické poště prostřednictvím serverů s protokoly SMTP a POP. Přístup k poště můžete buď zakázat úplně, nebo ho můžete povolit příležitostně.

Zabránění v přístupu pomocí protokolu SMTP

Pokud nechcete, aby někdo mohl používat protokol SMTP k distribuci elektronické pošty z vašeho systému nebo do vašeho systému, měli byste zakázat spuštění serveru SMTP.

Server SMTP je předvoleně konfigurován tak, aby se automaticky spustil při spuštění TCP/IP. Jestliže plánujete, že vůbec nebudete používat server SMTP, nekonfigurujte ho na vašem systému (ani nedovolte nikomu jinému, aby ho konfiguroval).

Zabránění protokolu SMTP, aby se spustil při spuštění TCP/IP:

Protokol SMTP chcete občas používat, ale chcete omezit počet přístupů, který uživatelé mají k serveru SMTP.

Chcete-li zabránit automatickému spuštění úloh serveru SMTP při spuštění TCP/IP, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Zrušte označení **Spustit při spuštění TCP/IP**.

Zabránění v přístupu k portům SMTP:

Chcete-li zabezpečit server SMTP (Simple Mail Transfer Protocol) proti neznámým aplikacím, můžete zakázat přístup k portům protokolu SMTP.

Pokud chcete zabránit ve spuštění protokolu SMTP a současně nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například soketovou aplikaci, k portu, který systém obvykle používá pro SMTP, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Vlastnosti**.

3. V okně Konfigurace TCP/IP - Vlastnosti klepněte myší na kartu **Omezení portu**.
4. Na stránce Omezení portu klepněte myší na **Přidat**.
5. Na stránce Přidat omezení portu zadejte tato nastavení:
   - **Jméno uživatele**: Zadejte jméno chráněného uživatelského profilu v systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port pro určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.
   - **Počáteční port**: 25
   - **Koncový port**: 25
   - **Protokol**: TCP
6. Klepněte na tlačítko **OK** a přidejte omezení.
7. Na stránce **Omezení portu** klepněte myší na **Přidat** a opakujte proceduru pro protokol UDP.
8. Klepněte myší na **OK**, uložte omezení portu a uzavřete okno **Konfigurace TCP/IP - Vlastnosti**. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.

Pozastavení front služeb SNADS:

Distribuční fronty služeb SNADS (Systems Network Architecture Distribution Services) používané aplikací SMTP k distribuci pošty lze pozastavit. Tím získáte další ochranu omezující distribuci pošty.

Chcete-li pozastavit distribuční fronty, zadejte ve znakově orientovaném rozhraní následující příkazy:

```
HLDDSTQ  DSTQ(QSMTPQ)PTY(*NORMAL)
HLDDSTQ  DSTQ(QSMTPQ)PTY(*HIGH)
```

Související pojmy

“Koncepce elektronické pošty” na stránce 2
V dnešní době jste závislí na elektronické poště jako na základním pracovním nástroji. Operační systém i5/OS používá protokoly, jako například SMTP (Simple Message Transfer Protocol) a POP (Post Office Protocol), aby byly vaše e-maily přijímány a odesílány po síti hladce a efektivně.

Řízení přístupu pomocí protokolu POP

Pokud chcete, aby nikdo nemohl používat protokol POP za účelem přístupu k systému, měli byste zakázat spuštění POP serveru.

Jestliže plánujete, že vůbec nebudete používat server POP, nekonfigurujte ho na vašem systému (ani nedovolte nikomu jinému, aby ho konfiguroval).

Zabránění protokolu POP, aby se spustil při spuštění TCP/IP:

Protokol POP chcete občas používat, ale chcete omezit počet přístupů, který uživatelé mají k POP serveru.

POP server je standardně konfigurován tak, aby se automaticky spustil při spuštění TCP/IP. Chcete-li zabránit automatickému spuštění úloh serveru POP při spuštění TCP/IP, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Klepněte pravým tlačítkem myši na **POP** a vyberte **Vlastnosti**.
3. Zrušte označení **Spustit při spuštění TCP/IP**.

Zabránění v přístupu k portům POP:

Chcete-li zabezpečit server POP (Post Office Protocol) proti neznámým aplikacím, můžete zakázat přístup k portům protokolu POP.

Pokud chcete zabránit ve spuštění protokolu POP a současně nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například soketovou aplikaci, k portu, který systém obvykle používá pro POP, postupujte takto:

1. V produktu System i Navigator se připojte k vašemu systému a rozbalte **Síť → Servery → TCP/IP**.
2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Vlastnosti**.
3. V okně Konfigurace TCP/IP - Vlastnosti klepněte myší na kartu **Omezení portu**.
4. Na stránce Omezení portu klepněte myší na **Přidat**.
5. Na stránce Přidat omezení portu zadejte tato nastavení:
   - **Jméno uživatele**: Zadejte jméno chráněného uživatelského profilu v systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port pro určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.
   - **Počáteční port**: 110 995
   - **Koncový port**: 110 995
   - **Protokol**: TCP
6. Klepněte na tlačítko **OK** a přidejte omezení.
7. Na stránce Omezení portu klepněte myší na **Přidat** a opakujte proceduru pro protokol UDP.
8. Klepněte myší na **OK**, uložte omezení portu a uzavřete okno Konfigurace TCP/IP - Vlastnosti.

Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.

Konfigurace e-mailu

Chcete-li nastavit e-mail na vašem systému, musíte nakonfigurovat TCP/IP, nastavit server SMTP a POP server a spustit e-mailové servery.

Související pojmy

“Protokol SMTP v operačním systému i5/OS” na stránce 3
Protokol SMTP (Simple Mail Transfer Protocol) je protokol, který umožňuje operačnímu systému odesílat a přijímat e-mail.

“Plánování e-mailu” na stránce 9
Před nastavením e-mailu byste měli mít základní představu o tom, jakým způsobem jej budete na systému používat.

Přistupování k e-mailovým serverům prostřednictvím produktu System i Navigator

Produkt System i Navigator můžete použít ke konfigurování a správě e-mailových serverů s protokoly SMTP (Simple Mail Transfer Protocol) a POP (Post Office Protocol).

Chcete-li v prostředí produktu System i Navigator získat přístup k serverům s protokoly POP nebo SMTP, postupujte takto:

1. Dvakrát klepněte myší na složku **Client Access Express**.
2. Dvakrát klepněte myší na **System i Navigator**. Pokud používáte produkt System i Navigator poprvé, klepněte myší na ikonu **Nové připojení** a vytvořte spojení s vaším systémem.
3. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
4. Dvakrát klepněte myší na **SMTP** a otevřete dialog Vlastnosti SMTP nebo dvakrát klepněte myší na **POP** a otevřete dialog Vlastnosti POP.

Související pojmy

“Protokol POP v operačním systému i5/OS” na stránce 4
Server POP (Post Office Protocol) je e-mailové rozhraní implementované v operačním systému i5/OS. Jedná se o Post Office Protocol verze 3.

Konfigurování TCP/IP pro e-mail

Předtím než nakonfigurujete e-mail ve vašem systému, musíte nastavit TCP/IP.

Při první konfiguraci e-mailu ve vašem systému postupujte takto: Jestliže již máte v systému nakonfigurován TCP/IP, můžete pokračovat přímo krokem Konfigurování serverů SMTP a POP pro e-mail.

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Konfigurace TCP/IP** .
2. Klepněte pravým tlačítkem myši na **Rozhraní** a zvolte **Nové rozhraní** a typ sítě, kterou nové rozhraní zastupuje. Chcete-li vytvořit nové rozhraní TCP/IP, postupujte podle pokynů průvodce. Průvodce vás požádá o tyto informace:
   - Typ připojení.
   - Hardwarový prostředek.
   - Popis linky.
   - IP adresa.
   - Hostitelské jméno.
   - Jméno domény.

     Hostitelské jméno a jméno domény, které použijete pro průvodce, vytváří vaše plně kvalifikované jméno domény. SMTP vyžaduje plně kvalifikované jméno domény, aby byla umožněna komunikace s ostatními hostiteli SMTP.

     Pokud je například jméno lokálního hostitele ASHOST a jméno lokální domény DOMAIN.COMPANY.COM, je plně kvalifikované jméno domény ASHOST.DOMAIN.COMPANY.COM.
   - Servery, které je třeba spustit.
3. Jakmile skončíte s tímto průvodcem, klepněte pravým tlačítkem myši na **TCP/IP** a vyberte **Vlastnosti**. Objeví se dialog Vlastnosti TCP/IP.
4. Klepněte myší na kartu **Tabulka hostitelů**.
5. Klepněte myší na **Přidat**. Objeví se dialog Záznam v tabulce hostitelů TCP/IP.
6. Zadejte IP adresu a hostitelské jméno, které jste použili v průvodci novým rozhraním TCP/IP.
7. Klepněte myší na **OK** a uzavřete dialog Záznam v tabulce hostitelů TCP/IP.
8. Klepněte myší na **OK** a uzavřete dialog Vlastnosti TCP/IP.

Související pojmy

“Určování problémů týkajících se e-mailu” na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Související úlohy

“Konfigurování serverů SMTP a POP pro e-mail”
Chcete-li používat e-mail, musíte nakonfigurovat servery SMTP a POP ve vašem systému.

Konfigurování serverů SMTP a POP pro e-mail

Chcete-li používat e-mail, musíte nakonfigurovat servery SMTP a POP ve vašem systému.

Poznámka: Jak server SMTP, tak POP server musí být správně nakonfigurovány.

Související pojmy

“Protokol POP v operačním systému i5/OS” na stránce 4
Server POP (Post Office Protocol) je e-mailové rozhraní implementované v operačním systému i5/OS. Jedná se o Post Office Protocol verze 3.

Související úlohy

“Konfigurování TCP/IP pro e-mail”
Předtím než nakonfigurujete e-mail ve vašem systému, musíte nastavit TCP/IP.

Konfigurace serveru SMTP

Jakmile nakonfigurujete TCP/IP, systém automaticky nakonfiguruje SMTP. Jediné, co musíte ještě udělat, je změnit několik vlastností SMTP, abyste zajistili, že server SMTP bude s elektronickou poštou správně pracovat.

Chcete-li změnit vlastnosti SMTP, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Chcete-li nastavit hodnoty pole označené ve sloupci Pak proveďte tuto akci, klepněte na karty vypsané v následující tabulce.

Klepněte na tuto kartu	Pak proveďte tuto akci
Obecné	Vyberte **Spustit při spuštění TCP/IP**.[1]
Obecné	V poli **Velikost pro rozdělení zprávy** vyberte volbu **Žádné maximum**.
Obecné	Máte-li směrovač pošty, zadejte jméno směrovače pošty, například mailrouter.company.com. Jméno směrovače pošty je jménem systému, kam SMTP směruje poštu v případě, že elektronická pošta není lokální poštou. Další informace naleznete v nápovědě k produktu System i Navigator.
Obecné	Jestliže máte nastaven firewall, vyberte **Předat odchozí poštu směrovači přes firewall**.
Obecné	Jestliže si vyměňujete elektronickou poštu se servery Domino, vymažte pole **Interpretovat znak procenta jako směrovací znak**.
Obecné	Pokud chcete předat veškerý nelokální e-mail na další server SMTP, zadejte v poli **Předávání domény poštovního rozbočovače** plně kvalifikovaný jméno domény výměníku pošty.
Obecné	Chcete-li, aby server SMTP podporoval znaky LF, CR nebo CRLF, vyberte volbu **Povolit přívod holého vedení**. Chcete-li, aby server SMTP podporoval pouze znak CRLF, odznačte zaškrtávací políčko **Povolit přívod holého vedení**.
Automatická registrace	Pokud pro odesílání elektronické pošty používáte příkaz SNDDST a pro přijímání příkaz RCVDST, a zároveň používáte adresování SNADS namísto internetového adresování, zaškrtněte políčko **Automaticky přidat vzdálené uživatele do systémového adresáře**.
Automatická registrace	Pokud pro odesílání elektronické pošty používáte příkaz SNDDST a pro přijímání příkaz RCVDST, klepněte na **Systémová tabulka aliasů** v poli **Přidat uživatele do**.

[1] Tato změna se uplatní při dalším spuštění serveru SMTP.

4. Klepněte myší na **OK** a potvrďte změny.

Související úlohy

"Ověření lokálního a předávaného e-mailu" na stránce 23
Před nevyžádanou poštou (spamem) se naní můžete chránit tak, že budete vyžadovat ověření při odesílání e-mailu na vašem serveru. Pokud chcete zakázat předávání zpráv, nemůžete vyžadovat ověření. Je doporučeno, abyste nastavili ověření pro váš server.

Povolení protokolu SSL mezi serverem SMTP a klientem v přijímajícím systému:

Pokud chcete povolit protokol SSL mezi serverem SMTP a klientem v přijímajícím systému, postupujte následujícím způsobem. Předpokládá se, že na serveru SMTP byl vytvořen certifikát serveru.

Aby bylo možné provést tuto úlohu, ujistěte se, že jste připojeni k přijímacímu systému.

Spuštění a konfigurace DCM

1. Ve vašem webovém prohlížeči se připojte k serveru SMTP: http://*váš_systém*: 2001/
2. Na stránce Úlohy i5/OS (Úlohy i5/OS) vyberte **Digital Certificate Manager** a poté klepněte na **Výběr úložiště certifikátů**.
3. Na stránce Výběr úložiště certifikátů, vyberte ***SYSTEM** a klepněte na **Pokračovat**.
4. Na stránce Úložiště certifikátů a heslo zadejte heslo vašeho úložiště certifikátů.

5. Rozbalte **Správa aplikací → Aktualizace přiřazení certifikátu** a vyberte **Server**.
6. Vyberte **server i5/OS TCP/IP SMTP** a v případě potřeby aktualizace přiřazení certifikátu klepněte na **Aktualizovat přiřazení certifikátu**.

Konfigurace serveru SMTP

Chcete-li povolit podporu SSL, nastavte pomocí příkazu CHGSMTPA (Změna atributů SMTP) parametr ALWAUTH buď na hodnotu *LCLRLY, nebo *RELAY.

- Pokud nastavíte tento parametr na hodnotu *RELAY, bude použití protokolu SSL podporováno pouze u e-mailových zpráv odeslaných z jiného serveru SMTP.
- Jestliže nastavíte tento parametr na hodnotu *LCLRLY, budou povoleny také parametry VFYMSFMSG (Verify MSF messages) a VFYFROMUSR (Verify from user). Tato předvolba může také způsobit odmítnutí určitých e-mailových zpráv. Určete, zda chcete povolit podporu takového odmítnutí.

Konfigurace klienta SMTP

Klienta SMTP v systému System i je třeba nakonfigurovat tak, aby se mohl přihlásit do přijímacího serveru SMTP v systému System i. K přidání položky do hostitelského ověřovacího seznamu použijte příkaz jazyka CL ADDSMTPLE (Přidat záznam do seznamu SMTP):

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(yoursystem.realm.com) USERNAME(receiver) PASSWORD(xxxx)
```

Jméno hostitele, které je uloženo velkými písmeny, musí odpovídat e-mailové adrese. Je-li e-mailová adresa myemail@yoursystem, musí být přidána tato položka:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(YOURSYSTEM) USERNAME(receiver) PASSWORD(xxxx)
```

Povolení protokolu SSL mezi serverem SMTP a klientem v odesílacím systému:

Aby bylo možné provést tuto úlohu, musíte být připojeni k odesílacímu systému.

1. Ve vašem webovém prohlížeči se připojte k serveru SMTP: http://*váš_systém*: 2001/
2. Na stránce Úlohy i5/OS (Úlohy i5/OS) vyberte **Digital Certificate Manager** a poté klepněte na **Výběr úložiště certifikátů**.
3. Na stránce Výběr úložiště certifikátů, vyberte ***SYSTEM** a klepněte na **Pokračovat**.
4. Na stránce Úložiště certifikátů a heslo zadejte heslo vašeho úložiště certifikátů a klepněte na tlačítko **Pokračovat**. Pokud nemáte certifikát uživatele nebo chcete certifikát uživatele vytvořit, proveďte kroky 5 až 8; jinak přejděte na krok 9.
5. Na stránce Vytvoření certifikátu vyberte **Certifikát uživatele** a klepněte na tlačítko **Pokračovat**.
6. Na stránce Vytvoření certifikátu uživatele zadejte do povinných polí informace o certifikátu a klepněte na tlačítko **Pokračovat**.
7. V okně Potenciální narušení skriptování klepněte na **Ano**.
8. Na stránce Vytvoření certifikátu uživatele klepněte na tlačítko **OK**. Systém bude používat certifikát uživatele klienta.
9. Rozbalte **Správa aplikací → Aktualizace přiřazení certifikátu**, vyberte **Certifikát serveru nebo klienta**.
10. Na obrazovce Aktualizace přiřazení certifikátu vyberte **Klient** a klepněte na tlačítko **Pokračovat**.
11. Vyberte **Klient i5/OS TCP/IP** a klepněte na tlačítko **Aktualizovat přiřazení certifikátu**.

Instalace certifikační autority příjemce na systému odesílatele:

Pokud je digitální certifikát příjemce vydán certifikační autoritou (CA), která je pro systém odesílatele neznámá, nainstalujte digitální certifikát pro certifikační autoritu v systému odesílatele.

Export certifikátu lokální CA a jeho odeslání do systému odesílatele.

Předpokládáme, že certifikační autorita je lokální, ačkoliv tuto proceduru můžete použít pro export jakéhokoliv certifikátu CA, který není znám v systému odesílatele.

Chcete-li exportovat lokální CA, postupujte takto:

1. Klepněte na **Výběr úložiště certifikátů** a vyberte **Lokální vydavatel certifikátů (CA)**. Klepněte na **Pokračovat**.
2. Na stránce Úložiště certifikátů a heslo, zadejte heslo.
3. Rozbalte **Správa lokální CA → Export** a vyberte **Soubor - Export do souboru**. Klepněte na **Pokračovat**.
4. Na stránce Export certifikátu, zadejte umístění adresáře a názvu souboru, kam bude uložen certifikát CA. Pokud adresář dosud neexistuje, použijte příkaz mkdir a adresář vytvořte.
5. Na stránce Export certifikátu byl úspěšný, klepněte na **OK**.
6. Chcete-li poslat certifikát CA ze systému příjemce do systému odesílatele, použijte FTP v režimu ASCII.

Instalace certifikátu CA v systému odesílatele

1. Na stránce Výběr úložiště certifikátů, vyberte ***SYSTEM** a klepněte na **Pokračovat**.
2. Na stránce Úložiště certifikátů a heslo, zadejte vaše heslo a klepněte na **Pokračovat**.
3. Rozbalte **Správa certifikátů → Import certifikátů**, vyberte **Vydavatel certifikátu (CA)** a klepněte na **Pokračovat**.
4. Na stránce Import certifikátu vydavatele certifikátů (CA), zadejte adresář, kde je uložen certifikát CA příjemce. Klepněte na **Pokračovat**.
5. Přiřaďte vašemu certifikátu popisek certifikátu a klepněte na **Pokračovat**. Zobrazí se zpráva: Certifikát byl naimportován.
6. Klepněte na **OK**.

Konfigurace POP serveru

Server POP (Post Office Protocol) musíte nakonfigurovat předtím, než ho budete používat k doručování pošty klientům POP.

POP server doručuje poštu klientovi POP ze schránky elektronické pošty v případě, že o to klient POP požádá. Aby byl váš systém plně připraven na používání elektronické pošty, je třeba nakonfigurovat POP server.

Při konfiguraci POP serveru pro poštovní programy, jako Netscape Mail nebo Eudora Pro, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Dvakrát klepněte myší na **POP**.
3. Prostudujte si níže uvedenou tabulku a nastavte příslušné parametry.

Klepněte na tuto kartu	**Pak proveďte tuto akci**
Obecné	Vyberte **Spustit při spuštění TCP/IP**.
Obecné	Pokud chcete povolit jak TLS/SSL tak nezabezpečené POP relace, vyberte volbu **Zabezpečené i nezabezpečené** v poli **Podpora SSL, která bude spuštěna se serverem**.
Konfigurace	V poli **Velikost pro rozdělení zprávy** vyberte volbu **Žádné maximum**.
Konfigurace	Jestliže se klienti POP přihlašují přes komutované linky a dostávají obsáhlou poštu, zvyšte **hodnotu časového limitu nečinnosti**.
Mapování	Vyberte **Použít pouze v případě, je-li uveden nepodporovaný CCSID**.

4. Klepněte myší na **OK** a potvrďte změny.

Přidružení certifikátu k POP serveru:

Proveďte tuto úlohu v případě, že jste nepřiřadili certifikát k aplikaci POP serveru během vytváření lokální CA (Certificate Authority) nebo pokud jste váš systém nakonfigurovali tak, že požaduje certifikát od veřejné CA.

1. Spusťte IBM Digital Certificate Manager. Pokud potřebujete získat nebo vytvořit certifikáty či jinak nastavit nebo změnit váš systém certifikátů, postupujte takto. Informace o nastavení systému certifikátů maleznete v tématu Konfigurace DCM.
2. Klepněte na **Výběr úložiště certifikátů**.
3. Vyberte ***SYSTEM**. Klepněte na **Pokračovat**.
4. Zadejte příslušné heslo pro úložiště cerifikátů *SYSTEM. Klepněte na **Pokračovat**.
5. Poté, co se znovu nahraje levé navigační menu, rozbalte **Správa aplikací**.
6. Klepněte na **Aktualizovat přiřazení certifikátu**.
7. Vyberte **Aplikace serveru**. Klepněte na **Pokračovat**.
8. Vyberte **i5/OS TCP/IP POP Server**.
9. Chcete-li přiřadit certifikát k tomuto POP serveru, klepněte na **Aktualizovat přiřazení certifikátu**.
10. Vyberte ze seznamu certifikát, který chcete přiřadit k serveru.
11. Klepněte na **Přiřadit nový certifikát**.
12. Poté co dokončíte nastavení certifikátů pro POP server, klepněte na **Hotovo**.

Zaregistrování uživatelů e-mailu

Abyste mohli zaregistrovat uživatele e-mailu, musíte vytvořit uživatelské profily.

Uživatelské profily představují způsob, jakým systém i5/OS identifikuje adresáta nebo odesílatele e-mailu. Všichni uživatelé, kteří mají být součástí e-mailového systému, musí mít v systému uživatelský profil.

Tím, že vytvoříte pro každého uživatele uživatelský profil, zapíšete uživatele automaticky do systémového distribučního adresáře. Protokol SMTP podle systémového distribučního adresáře určuje, kam doručit lokální elektronickou poštu.

Chcete-li vytvořit uživatelské profily pro uživatele elektronické pošty SNADS a POP, použijte tento postup:

1. V produktu System i Navigator rozbalte ***systém*** **→ Uživatelé a skupiny**.
2. Klepněte pravým tlačítkem myši na **Všichni uživatelé** a vyberte **Nový uživatel**.
3. Napište jméno uživatele a jeho heslo.

   Poznámka: Uživatelé POP použijí toto heslo, aby získali přístup do své schránky elektronické pošty POP.
4. Klepněte myší na tlačítko **Schopnosti**.
5. Klepněte myší na tlačítko **Oprávnění**. Ujistěte se, že třída oprávnění je **Uživatel**.
6. Klepněte na **OK**.
7. Klepněte myší na tlačítko **Osobní**.
8. Klepněte myší na kartu **Pošta**.
9. Zvolte **Úroveň služeb pošty**.
   - Jestliže je váš uživatel uživatelem SNADS, vyberte **Uživatelský rejstřík**.
   - Jestliže je váš uživatel uživatelem pošty POP3, vyberte volbu **Systémová schránka elektronické pošty**.
10. Zvolte **Preferovaný typ adresy**.
    - Jestliže je váš uživatel uživatelem SNADS, vyberte **ID uživatele a adresa**.
    - Jestliže je váš uživatel uživatelem pošty POP3, vyberte volbu **Jméno SMTP**.
11. Ověřte, že se pro doménu SMTP elektronické pošty zobrazí požadované jméno domény. Předvolené jméno je obvykle správné, ale jestliže máte více lokálních domén, budete je možná muset změnit.
12. Klepněte na **OK**. Registrujete-li uživatele SNADS, je jeho registrace dokončena. Pokud registrujete uživatele POP, který bude používat i5/OS POP server pouze k získávání e-mailu, pokračujte dalším krokem.

13. Klepněte myší na tlačítko **Úlohy**.
14. Klepněte myší na kartu **Spuštění relace**.
15. V poli **Počáteční menu** vyberte **Odhlásit**. Toto nastavení způsobí automatické odhlášení uživatele při každém pokusu o přihlášení k systému s jiným požadavkem, než je získání pošty nebo změna hesla.
16. Klepněte na **OK**.
17. Klepněte na **OK**.
18. Opakujte tyto kroky, dokud nebudou mít všichni uživatelé elektronické pošty svůj uživatelský profil.

Související pojmy

"Odeslání a přijetí e-mailu" na stránce 28
Váš systém je poštovní server a jsou na něm zapsáni e-mailoví uživatelé (uživatelé SNADS, POP nebo Lotus). Pomocí klienta POP nebo SNADS mohou tito uživatelé odesílat, přijímat nebo číst e-mail.

Související úlohy

"Odeslání e-mailu pomocí distribučních služeb SNA" na stránce 30
E-mail z vašeho systému můžete odeslat pomocí klientského programu SNDAS (Systems Network Architecture distribution services). Odesilatel e-mailu musí být lokální uživatel SNADS.

Spuštění a zastavení e-mailových serverů

Spuštěním požadovaných serverů se ujistíte, že vše řádně funguje a že se provedly veškeré zadané změny konfigurace. Někdy bývá nutné servery restartovat. To lze provést tak, že servery zastavíte a potom provedete kroky potřebné pro jejich restartování.

Související úlohy

"Kontrola poštovních serverů" na stránce 34
Jedním z nejčastějších problémů týkajících se e-mailu je ten, že nejsou spuštěny správné servery. Před použitím poštovních serverů ověřte jejich stav a ujistěte se, že jsou všechny spuštěné.

Spuštění e-mailových serverů

Spuštěním serverů způsobíte, že se z vašeho systému stane e-mailový server se zaregistrovanými e-mailovými uživateli.

Při spouštění serverů postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť**.
2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Vlastnosti**. Otevře se dialogové okno Konfigurace TCP/IP - Vlastnosti.
   - Jestliže je stav TCP/IP Spuštěno, klepněte myší na **OK** a pokračujte dalším krokem.
   - Pokud tomu tak není, klepněte myší na **Zrušit** a tím uzavřete dialog Konfigurace TCP/IP - Vlastnosti. Potom klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Spustit**. Po dokončení operace klepněte na tlačítko **OK**.
3. Rozbalte **Servery** → **TCP/IP**. Nejsou-li servery SMTP a POP spuštěné, spustíte je takto:
   a. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Spustit**.
   b. Klepněte pravým tlačítkem myši na **POP** a vyberte **Spustit**.
4. Otevřete znakově orientované rozhraní a zadáním příkazu STRMSF spusťte funkci MSF (Mail Server Framework).
5. Používáte-li SNADS, spusťte subsystém QSNADS zadáním příkazu STRSBS QSNADS.

Nyní, po spuštění serverů, je váš systém e-mailovým serverem se zaregistrovanými e-mailovými uživateli.

Zastavení e-mailových serverů

K zastavení e-mailových serverů můžete použít produkt System i Navigator.

Jestliže chcete zastavit servery, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.Jsou-li servery SMTP a POP spuštěny, zastavíte je takto:
   a. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Zastavit**.
   b. Klepněte pravým tlačítkem myši na **POP** a vyberte **Zastavit**.
2. Otevřete znakově orientované rozhraní a zadáním příkazu ENDMSF zastavte funkci MSF (Mail Server Framework).
3. Používáte-li SNADS, zadejte příkaz ENDSBS QSNADS, kterým ukončíte subsystém QSNADS.

Konfigurování profilu připojení po komutované lince

Jestliže nemáte podporu AT&T Global Network, musíte nejprve nakonfigurovat profil připojení pošty.

Jestliže chcete ručně vytvořit profil připojení po komutované lince, postupujte takto:

Poznámka: Máte-li podporu AT&T Global Network support, můžete přejít na téma Konfigurování průvodce připojením ISP po komutované lince.

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem myši na **Profily připojení příjemců** a vyberte **Nový profil**.
3. Vyberte **PPP** pro **Typ protokolu**.
4. Vyberte **Komutovaná linka** pro **Typ připojení**.
5. Rozbalte **Konfigurace TCP/IP** a zvolte **Připojení**.
6. Rozbalte **Servery** → **TCP/IP**.
7. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
8. Klepněte myší na kartu **Plánovač**. Vyberte zaškrtávací políčko **Spustit plánovač při spuštění SMTP** a zadejte profil připojení, který jste vytvořili.
9. Klepněte myší na stránku ETRN a vyberte zaškrtávací políčko **Support ETRN (Dial-up mail retrieval)**. Klepněte myší na **Přidat** a zadejte jméno domény pro adresu odchozího serveru ISP.
10. Aktivujte ochrannou bariéru a ukažte myší na odchozí poštovní server ISP.
11. Pokračujte v práci s průvodcem a nastavte nové Připojení ISP po komutované lince.

Související úlohy

"Konfigurování průvodce připojením ISP po komutované lince"
Před odesláním velkého množství elektronické pošty prostřednictvím poskytovatele služeb Internetu (ISP) pomocí plánovače protokolu SMTP musíte nakonfigurovat profil připojení po komutované lince.

Konfigurování průvodce připojením ISP po komutované lince

Před odesláním velkého množství elektronické pošty prostřednictvím poskytovatele služeb Internetu (ISP) pomocí plánovače protokolu SMTP musíte nakonfigurovat profil připojení po komutované lince.

Při konfiguraci profilu připojení ISP po komutované lince můžete použít průvodce připojením po komutované lince prostřednictvím ISP.

Nezbytné předpoklady:

Pokud nemáte podporu AT&T Global Network, přečtěte si nejdříve téma Konfigurování profilu připojení po komutované lince, kde najdete úvodní informace nezbytné pro konfiguraci. Průvodce připojením vám poskytne IP adresu poštovních serverů (SMTP a POP), jejich přiřazené jméno domény, jméno účtu a heslo.

Jestliže chcete spustit průvodce a nakonfigurovat plánovač SMTP, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem myši na **Profily připojení odesílatelů** a vyberte **Nové telefonické připojení do AT&T Global Network**.

3. V dialogovém okně Vítejte klepněte myší na **Další**.
4. V dialogovém okně **Typ aplikačního serveru** vyberte **Aplikace vzájemné výměny pošty** a klepněte myší na **Další**.
5. Pokračujte v práci s průvodcem a nastavte nové telefonické připojení do AGN.

Poté, co jste nakonfigurovali připojení po komutované lince, jste připraveni přejít k tématu Rozvržení dávkových úloh e-mailu ISP.

Související úlohy

"Konfigurování profilu připojení po komutované lince" na stránce 20
Jestliže nemáte podporu AT&T Global Network, musíte nejprve nakonfigurovat profil připojení pošty.

"Plánování dávkových úloh e-mailu ISP"
Chcete-li omezit dobu potřebnou k vytvoření připojení, naplánujte úlohy zpracování pošty po komutované lince tak, abyste se připojovali k ISP v pravidelných intervalech. Potom pomocí plánovače SMTP nastavte časové intervaly, v nichž se má systém připojovat k ISP a odesílat e-mail.

Plánování dávkových úloh e-mailu ISP

Chcete-li omezit dobu potřebnou k vytvoření připojení, naplánujte úlohy zpracování pošty po komutované lince tak, abyste se připojovali k ISP v pravidelných intervalech. Potom pomocí plánovače SMTP nastavte časové intervaly, v nichž se má systém připojovat k ISP a odesílat e-mail.

Nezbytné předpoklady:

Jestliže chcete nakonfigurovat připojení, postupujte podle pokynů v tématu Průvodce připojením ISP po komutované lince.

Pokud chcete nastavit plánovač SMTP pro odesílání e-mailu poskytovateli služeb sítě Internet (ISP), postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Klepněte myší na kartu **Plánovač**.
4. Vyberte zaškrtávací políčko **Spustit plánovač při spuštění SMTP**.
5. Vyberte **Profil dvoubodového připojení**, který jste nakonfigurovali pomocí průvodce telefonickým připojením do AT&T Global Network, nebo vyberte ručně konfigurovaný **Profil dvoubodového připojení**.
6. U položky **Interval přenosu pošty** nastavte počet minut, po kterých vždy SMTP bude doručovat poštu.
7. Jestliže ISP není v síti AT&T Global Network, vyberte zaškrtávací políčko **Vydat ETRN při připojování na vzdálený server**.
8. Zadejte IP adresu serveru pro server příchozí pošty v síti ISP. Poté vyplňte pole Registrovaná hostitelská doménu ISP, pro kterou server SMTP vydá ETRN.
9. Klepněte na **OK**.

Související úlohy

"Konfigurování průvodce připojením ISP po komutované lince" na stránce 20
Před odesláním velkého množství elektronické pošty prostřednictvím poskytovatele služeb Internetu (ISP) pomocí plánovače protokolu SMTP musíte nakonfigurovat profil připojení po komutované lince.

"Konfigurace serveru SMTP pro vyzvedávání pošty po vytáčené lince (dial-up)"
Server SMTP (Simple Mail Transfer Protocol) můžete používat k přijímání pošty pro vzdálená pracoviště, která se připojují pomocí vytáčené linky.

Konfigurace serveru SMTP pro vyzvedávání pošty po vytáčené lince (dial-up)

Server SMTP (Simple Mail Transfer Protocol) můžete používat k přijímání pošty pro vzdálená pracoviště, která se připojují pomocí vytáčené linky.

Systém musí mít pevnou IP adresu a musí být registrován pomocí DNS. Každá hostitelská doména, pro kterou budou vzdálené servery připojené po vytáčené lince získávat poštu, musí mít v DNS také záznamy MX, odkazující na tento systém. Systém musí mít v lokální hostitelské tabulce pro tyto hostitelské domény také aliasy. Jestliže jsou vzdálené servery, připojené po vytáčené lince, spuštěny na operačním systému i5/OS, musí být tyto servery konfigurovány pro Rozvržení dávkových úloh e-mailů ISP.

Jestliže chcete přijímat požadavky e-mailů ze vzdálených poštovních serverů připojených po vytáčené lince, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Klepněte myší na kartu **ETRN**.
4. Vyberte zaškrtávací políčko **Podpora ETRN (Dial-up mail retrieval)**.
5. Klepněte myší na **Přidat** a zadejte jméno hostitele a domény ISP. Tuto proceduru je někdy nutné provést několikrát, pokud elektronickou poštu požaduje více poštovních serverů.
6. Klepněte na **OK**.

Související úlohy

"Plánování dávkových úloh e-mailu ISP" na stránce 21
Chcete-li omezit dobu potřebnou k vytvoření připojení, naplánujte úlohy zpracování pošty po komutované lince tak, abyste se připojovali k ISP v pravidelných intervalech. Potom pomocí plánovače SMTP nastavte časové intervaly, v nichž se má systém připojovat k ISP a odesílat e-mail.

Podpora vícenásobných domén

Server SMTP můžete nakonfigurovat tak, aby podporoval vícenásobné domény, a mohl tak hostit funkce ISP.

Aby mohl server SMTP hostit funkce ISP, je nutné, aby protokol SMTP fungoval ve více doménách. Klient SMTP použije tyto informace o konfiguraci, aby zjistil, ke kterému rozhraní se má připojit, když odesílá e-mail, a kterou poštu má pokládat za lokální (otevře a odešle ji sám) nebo kterou má předat poštovnímu démonovi s nakonfigurovanou bránou firewall.

1. V produktu System i Navigator rozbalte ***systém*** → **TCP/IP** → **Síť**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte myší na kartu **Vícenásobné domény**.
4. Klepněte myší na **Přidat** a zadejte domény a rozhraní, které chcete podporovat.
5. Klepněte na **OK**.

Související pojmy

"Nezbytné předpoklady pro e-mailový směrovač" na stránce 23
V tomto tématu se dozvíte, co je třeba provést před konfigurací e-mailového směrovače.

Zabezpečení e-mailu

Při zabezpečení e-mailu vám může pomoci použití bran firewall, vyhrazených přenosových bran a připojení a filtrování virů.

Je důležité podporovat na serveru SMTP (Simple Mail Transfer Protocol) bezpečné prostředí. Server SMTP a uživatele musíte třeba chránit před vnitřními a vnějšími překážkami.

Související pojmy

"Koncepce elektronické pošty" na stránce 2
V dnešní době jste závislí na elektronické poště jako na základním pracovním nástroji. Operační systém i5/OS používá protokoly, jako například SMTP (Simple Message Transfer Protocol) a POP (Post Office Protocol), aby byly vaše e-maily přijímány a odesílány po síti hladce a efektivně.

Související odkazy

Create and Send MIME E-mail (QtmsCreateSendEmail) API

Související informace

Zabezpečení e-mailu

Odesílání e-mailu přes směrovač nebo bránu firewall

Směrovač elektronické pošty je pomocným systémem, přes který SMTP doručuje poštu v případě, kdy nemůže najít přesnou IP adresu příjemce.

Směrovač elektronické pošty směruje elektronickou poštu na IP adresu nebo na další směrovač. Jestliže váš lokální server nedoručuje elektronickou poštu do systému, směrujte odchozí poštu do alternativního systému. Máte-li ochrannou bariéru, můžete ji použít jako směrovač.

Ještě před konfigurováním směrovače si přečtěte téma "Nezbytné předpoklady pro e-mailový směrovač".

Při nastavování směrovače postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Klepněte myší na kartu **Obecné**.
4. Zadejte jméno pro Směrovač pošty.

Jestliže chcete směrovat poštu přes ochrannou bariéru, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Klepněte myší na kartu **Obecné**.
4. Do pole **Směrovač pošty** zadejte jméno brány firewall, například FWAS400.company.com.
5. Vyberte **Postoupit odchozí poštu na směrovač pošty přes ochrannou bariéru**.

Nezbytné předpoklady pro e-mailový směrovač

V tomto tématu se dozvíte, co je třeba provést před konfigurací e-mailového směrovače.

Před konfigurováním e-mailového směrovače se seznamte s následujícími skutečnostmi:

- Zprostředkující server nemusí být operačním systémem i5/OS. Směrovač pošty vyžaduje pouze hostitelskou tabulku, která obsahuje všechny hostitelské servery, na něž potřebuje směrovač směrovat e-mail. Pokud je směrovačem pošty operační systém i5/OS, nevyžaduje žádnou konkrétní úroveň systému.
- Pro směrování mezi zdrojovým a cílovým serverem můžete nastavit pouze jeden zprostředkující server. Nemůžete včlenit směrovače pošty.
- Server SMTP musí být při spuštění schopen získat IP adresu pro směrovač pošty, a to buď z lokální hostitelské tabulky, nebo pomocí serveru DNS (Domain Name System). Jestliže server SMTP nemůže získat IP adresu pro směrovač pošty, potom server SMTP běží bez použití směrovače.
- Brána firewall klienta SMTP používá směrovač pošty k doručování e-mailu, který je určen pro hostitele mimo lokální (chráněnou) doménu. Aby mohla být doručena pošta, musí být směrovačem pošty server, jenž má oprávnění k doručování e-mailu přes bránu firewall. Také příjemci pošty, jejichž doména není v operačním systému i5/OS, jsou připojeni přes směrovač, pokud je zapnuta podpora brány firewall SMTP. Operační systém i5/OS V5R1 a novější podporuje více místních domén. Je možné nakonfigurovat více domén, které neposílají poštu přes bránu firewall.

  Související úlohy

  "Podpora vícenásobných domén" na stránce 22
  Server SMTP můžete nakonfigurovat tak, aby podporoval vícenásobné domény, a mohl tak hostit funkce ISP.

Ověření lokálního a předávaného e-mailu

Před nevyžádanou poštou (spamem) se naní můžete chránit tak, že budete vyžadovat ověření při odesílání e-mailu na vašem serveru. Pokud chcete zakázat předávání zpráv, nemůžete vyžadovat ověření. Je doporučeno, abyste nastavili ověření pro váš server.

Chcete-li povolit ověření pro váš server, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Klepněte na kartu **Authentizace** a nastavte hodnoty pole, které jsou označeny ve sloupci Pak proveďte tuto akci.

Klepněte na tuto kartu	Pak proveďte tuto akci
Autentizace	Chcete-li, aby server používal TLS/SSL k ověření lokálně a při předávání zpráv, vyberte **Vyžadovat TLS/SSL a autentizovat lokálně a při používání přenosové brány**.
Autentizace	Chcete-li, aby server používal TLS/SSL pouze k ověření při funkci předávání, vyberte **Vyžadovat TLS/SSL a autentizovat pouze přenosovou bránu**.
Autentizace	Pokud chcete povolit přihlášení na server SMTP pouze uživatelům, kteří jsou uvedeni v autorizovaném seznamu, vyberte **Ověřovat ID při lokálním doručení**.
Autentizace	Chcete-li, aby server SMTP povolil MSF funkce snap-in k odmítnutí e-mailu, který není ověřen, vyberte **Ověřit původce zpráv**.
Autentizace	Chcete-li, aby server SMTP ověřoval, zda e-mailová adresa odesílatele je uvedena v distribučním adresáři systému a zda tato adresa odpovídá, vyberte **Uživatelé** nebo **Uživatelé ne v přijatém seznamu**. Uživatelé, jejichž e-mailové adresy neodpovídají, jsou odmítnuti.

4. Klepněte myší na **OK** a potvrďte změny.

Související úlohy

"Omezení předávání zpráv" na stránce 25
Chcete-li lidem zabránit, aby používali váš e-mailový server pro spam nebo pro odesílání velkého množství hromadných e-mailů, můžete použít funkci pro omezení předávání k tomu, abyste určili, kdo může používat váš systém pro předávání zpráv. Avšak nemůžete ověřit váš e-mail, pokud omezíte předávání zpráv.

"Konfigurace serveru SMTP" na stránce 15
Jakmile nakonfigurujete TCP/IP, systém automaticky nakonfiguruje SMTP. Jediné, co musíte ještě udělat, je změnit několik vlastností SMTP, abyste zajistili, že server SMTP bude s elektronickou poštou správně pracovat.

Sledování odesílatele e-mailu

Nyní můžete nastavit server SMTP tak, aby odmítnul odesílatele e-mailu, který nemá autentizace. Kromě toho můžete nastavit funkce snap-in MSF (mail server framework) SMTP tak, aby odmítly e-mail, který není ověřený.

Aby bylo možné odmítnout neověřeného odesílatele nebo e-mail, je třeba povolit šifrování transakcí, to znamená protokoly TLS/SSL.

Odmítnutí odesílatele e-mailu, který není ověřen

Chcete-li odmítnout odesílatele e-mailu, kteří nejsou ověřeni, postupujte následujícím způsobem:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte na kartu **Autentizace**.
4. Pokud chcete ověřit všechny odesílatele e-mailu, v poli **Ověřit poštu od uživatele** vyberte **Všichni**. Pokud chcete ověřovat pouze uživatele, kteří nejsou v seznamu příjemců, vyberte možnost **Uživatelé, kteří nejsou v seznamu příjemců**.
5. Klepněte na **OK**.

Server SMTP zkontroluje, zda je odesílatel v systémovém distribučním adresáři a zda e-mailová adresa odpovídá některé adrese v tomto adresáři. Pokud zde není shoda, je uživatel odmítnut.

Odmítnutí e-mailu, který není ověřen

Chcete-li odmítnout e-mail, který není ověřen, postupujte následujícím způsobem:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte na kartu **Autentizace**.
4. V poli **Povolit autentizaci** vyberte možnost **Vyžadovat TLS/SSL a autentizovat lokálně a při používání přenosové brány**.
5. Vyberte **Ověřit původce zprávy MSF**.
6. Klepněte na **OK**.

Pokud tento e-mail nepochází z ověřeného zdroje, potom by měl být původcem zprávy uživatel, který vydal rozhraní QzmfCrtMailMsg() API. V opačném případě funkce snap-in SMTP tyto e-maily odmítnou.

Omezení předávání zpráv

Chcete-li lidem zabránit, aby používali váš e-mailový server pro spam nebo pro odesílání velkého množství hromadných e-mailů, můžete použít funkci pro omezení předávání k tomu, abyste určili, kdo může používat váš systém pro předávání zpráv. Avšak nemůžete ověřit váš e-mail, pokud omezíte předávání zpráv.

Při povolování předávání máte k dispozici šest voleb:

- Povolit všem předávat zprávy.
- Blokovat předané zprávy.
- Přijímat pouze zprávy předávané z blízkých domén.
- Přijímat pouze zprávy předávané z adres uvedených na seznamu.
- Přijímat zprávy předávané z blízkých domén i z adres na seznamu.
- Přijímat zprávy předávané z klientů POP po stanovenou dobu.

Předávání zpráv můžete nyní omezit pouze když vyberete volbu **Nebude provedeno TLS/SSL ani autentizace**. V produktu System i Navigator naleznete tuto volbu na stránce Autentizace, když zadáváte vlastnosti SMTP.

Chcete-li určit uživatele, kteří mohou odesílat elektronickou poštu na Internet, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte myší na kartu **Omezení přenosů**.
4. Vyberte požadované omezení předávání z nabízených voleb.

   Poznámka: Jestliže vyberete volbu **Přijmout pouze předané zprávy z blízkých domén** nebo **Přijmout předané zprávy jak z blízkých domén, tak z adres na seznamu** , budete muset klepnout myší na kartu **Obecné** a vypsat seznam blízkých domén, ze kterých předání přijímáte.
5. Klepněte na **OK**.

Související pojmy

"Řízení přístupu k e-mailu" na stránce 10
Měli byste řídit, kdo přistupuje k systému prostřednictvím e-mailu. Tím ochráníte svá data před svévolnými útoky.

Související úlohy

"Ověření lokálního a předávaného e-mailu" na stránce 23
Před nevyžádanou poštou (spamem) se naní můžete chránit tak, že budete vyžadovat ověření při odesílání e-mailu na vašem serveru. Pokud chcete zakázat předávání zpráv, nemůžete vyžadovat ověření. Je doporučeno, abyste nastavili ověření pro váš server.

"Společné použití funkce omezení přenosu a funkce omezení připojení" na stránce 26
Operační systém i5/OS umožňuje dokonalé řízení přístupů k e-mailovému serveru tím, že umožňuje používat funkci omezení přenosu společně s funkcí omezení připojení.

Související odkazy

Příjem zpráv předávaných z klientů POP (Post Office Protocol)

Jedna z voleb, které slouží k omezení přenosu, umožňuje klientům POP po určitou dobu po jejich přihlášení k serveru s protokolem POP přenášet zprávy pomocí protokolu SMTP.

Tato funkce se obecně nazývá POP před SMTP. Je zvláště užitečná v případě mobilních pracovníků používajících dynamické IP adresy, protože funkce bezpečnostní kontroly pro pevné IP adresy nejsou při kontrole dynamických IP adres účinné. Mobilnímu uživateli můžete povolit, aby po provedení autentizace na serveru s protokolem POP, mohl odesílat elektronickou poštu po předem stanovenou dobu (15 - 65535 minut), aniž by se musel znovu autentizovat.

Systém můžete například nakonfigurovat tak, aby vzdálení uživatelé měli povoleno přenášet zprávy přes server SMTP po dobu čtyř hodin (240 minut) po svém přihlášení k serveru s protokolem POP. V našem příkladu se mobilní pracovník přihlásí k serveru s protokolem POP, aby si stáhl poštu. Server POP si do fronty poznamená IP adresu uživatele a časový údaj. O hodinu později se uživatel rozhodne odeslat e-mailovou zprávu. Pokud uživatel odesílá zprávu přes SMTP, zkontroluje server frontu, aby si ověřil, že uživatel někdy v průběhu zadaného časového úseku provedl přístup k serveru s protokolem POP, aby si stáhl poštu. Po ověření uživatele server SMTP předá e-mailovou zprávu klientu SMTP, aby mohla být doručena příslušným příjemcům.

Poznámka: Chcete-li přísněji kontrolovat uživatele, kteří mají přístup k poštovnímu serveru, můžete použít funkci omezení přenosu společně s funkcí omezení připojení. Můžete například zabránit určité skupině uživatelů v připojení k vašemu poštovnímu serveru, ale určitým klientům POP v rámci této skupiny povolit elektronické odesílání zpráv přes server SMTP.

Chcete-li povolit klientům POP přenášet zprávy po stanovenou dobu, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte myší na kartu **Omezení přenosů**.
4. V poli **Povolit přenos zpráv**, vyberte **Zadaný**.
5. Vyberte volbu **Z klienta POP pro následující dobu trvání (15 - 65535)** a zadejte časový údaj, v němž uvedete počet minut, po který bude klient smět posílat poštu přes server SMTP.
6. Klepněte na **OK**.

Společné použití funkce omezení přenosu a funkce omezení připojení

Operační systém i5/OS umožňuje dokonalé řízení přístupů k e-mailovému serveru tím, že umožňuje používat funkci omezení přenosu společně s funkcí omezení připojení.

Můžete zabránit určité skupině uživatelů v připojení k poštovnímu serveru, ale určitým klientům POP v rámci této skupiny povolit elektronické odesílání zpráv přes server SMTP.

Víte například, že uživatelé v rámci určitého okruhu IP adres pravidelně odesílají spamy. Pro tyto adresy můžete omezit přístup k vašemu poštovnímu serveru. Některé z IP adres z tohoto okruhu však představují důvěryhodné uživatele systému i5/OS a vy byste chtěli těmto uživatelům s uživatelským profilem systému i5/OS povolit přenos zpráv po určitou dobu po jejich přihlášení k serveru POP.

Naštěstí můžete pomocí funkce omezení připojení omezit připojení pro určitý rozsah IP adres a zároveň pomocí funkce omezení přenosu povolit určitým důvěryhodným uživatelům (klientům POP) v rámci tohoto omezeného rozsahu adres odesílat e-maily přes server SMTP. Operační systém i5/OS nejprve zkontroluje, zda je systém nakonfigurován na povolení přenosu zpráv pro klienty POP po stanovenou dobu.Potom zkontroluje omezená připojení. Tato schopnost systému i5/OS umožňuje přesně regulovat, kdo může používat server SMTP k přenosu zpráv a kdo se může připojovat k vašemu poštovnímu serveru.

| Pokud se rozhodnete pro společné použití funkce omezení připojení a funkce omezení přenosu, budete potřebovat zadat
| OVRRJTNNL(*YES) (Seznam přepisu zamítnutí připojení) v příkazu CHGSMTPA typu CL (Změna atributů SMTP).
| Tento parametr umožní, aby funkce ověřování na serveru s protokolem POP přepsala konfiguraci omezení týkající se

připojení. Budete-li chtít, můžete omezení přenosu, které umožňuje klientům POP v rámci omezené skupiny používat váš poštovní server, později zrušit. V tomto případě budete potřebovat zadat OVRRJTNNL(*NO) na příkazu CHGSMTPA.

Související úlohy

"Omezení předávání zpráv" na stránce 25
Chcete-li lidem zabránit, aby používali váš e-mailový server pro spam nebo pro odesílání velkého množství hromadných e-mailů, můžete použít funkci pro omezení předávání k tomu, abyste určili, kdo může používat váš systém pro předávání zpráv. Avšak nemůžete ověřit váš e-mail, pokud omezíte předávání zpráv.

"Zákaz připojení"
Chcete-li zabezpečit systém, můžete zabránit připojení uživatelů, kteří by mohli zneužít váš e-mailový server.

Související odkazy

Příkaz CHGSMTPA (Změna atributů SMTP)

Zákaz připojení

Chcete-li zabezpečit systém, můžete zabránit připojení uživatelů, kteří by mohli zneužít váš e-mailový server.

K vašemu serveru se mohou připojit nežádoucí uživatelé a odeslat nevyžádanou poštu. Tato nevyžádaná pošta zabere velkou část cyklů a prostoru. Jestliže váš systém umožní ostatním přenášet nevyžádanou elektronickou poštu, mohou ostatní servery zablokovat poštu, která přichází z vašeho systému.

Můžete zadat IP adresy známých nežádoucích uživatelů nebo se můžete připojit k hostiteli, který obsahuje server RBL (Realtime Blackhole List). Tyto servery RBL poskytují seznamy známých IP adres, které odesílají nevyžádané e-maily.

Jestliže chcete zadat známé IP adresy nebo hostitele s RBL, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte myší na stránku Omezení připojení.
4. Klepněte myší na **Přidat** a přidejte hostitelská jména serverů s RBL (Realtime Blackhole List), které byste chtěli použít.
5. Klepněte myší na **Přidat** a přidejte specifické IP adresy pro omezení připojení.
6. Klepněte na **OK**.

Související pojmy

"Řízení přístupu k e-mailu" na stránce 10
Měli byste řídit, kdo přistupuje k systému prostřednictvím e-mailu. Tím ochráníte svá data před svévolnými útoky.

Související úlohy

"Společné použití funkce omezení přenosu a funkce omezení připojení" na stránce 26
Operační systém i5/OS umožňuje dokonalé řízení přístupů k e-mailovému serveru tím, že umožňuje používat funkci omezení přenosu společně s funkcí omezení připojení.

Filtrování e-mailu jako prevence šíření virů

Abyste omezili šíření virů, které mohou proniknout do poštovních serverů, můžete vytvořit filtry, které budou v příchozím e-mailu kontrolovat určitý předmět, typ nebo jméno souboru a adresu odesílatele. Elektronická pošta může být potom pokládána za ověřenou nebo může být vyřazena.

Při filtrování virů se podezřelé e-maily automaticky uloží nebo vyřadí na základě parametrů zadaných administrátorem. Elektronická pošta může být ″filtrována″ podle některých z těchto kritérií:

1. **Adresa** - jednotlivci nebo domény.
2. **Předmět** - ILOVEYOU.
3. **Jméno přípony** - lovebug.vbs nebo *.vbs.
4. **Typ MIME** - image/* nebo image/jpg.

Hodnoty mohou obsahovat zástupné znaky. Jedním ze zástupných znaků je hvězdička (*), která určuje, že na místě zástupného znaku může být jeden nebo více libovolných znaků. Například zápis *.vbs by mohl být použit pro kontrolu jmen souborů s příponou .vbs. Zápis *@us.ibm.com filtruje veškerou poštu od IBM ve Spojenýcch státech a filtr image/* filtruje typ obrazu pro všechny podtypy.

Při vytváření filtru postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Vyberte stránku Filtry.
4. Vyberte **Uchovat zprávy** nebo **Vyřadit zprávy**. Pomocí volby **Uchovat zprávy** uložíte kopii zprávy, která nebude doručena příjemci.
5. Klepněte myší na **Přidat** a určete kritéria zprávy, která identifikují možný virus. Zprávy, které budou odpovídat těmto kritériím, nebudou doručeny příjemci.
6. Klepněte myší na **OK** a uložte změny.

Kromě těchto nástrojů byste měli použít další antivirová opatření.

Odeslání a přijetí e-mailu

Váš systém je poštovní server a jsou na něm zapsáni e-mailoví uživatelé (uživatelé SNADS, POP nebo Lotus). Pomocí klienta POP nebo SNADS mohou tito uživatelé odesílat, přijímat nebo číst e-mail.

K odesílání e-mailu z programu operačního systému i5/OS mohou uživatelé používat rozhraní Send MIME Mail (QtmmSendMail) API nebo Create and Send MIME Email (QtmsCreateSendEmail) API. Pomocí rozhraní QtmsCreateSendEmail API mohou uživatelé podepsat a zašifrovat dokument MIME za použití protokolu secure/MIME, což je zabezpečená verze protokolu MIME. Při odesílání e-mailu prostřednictvím programů se dává přednost rozhraní QtmsCreateSendEmail API.

Kromě toho mohou uživatelé odesílat a přijímat e-mail následujícími různými způsoby:

Související pojmy

“Koncepce elektronické pošty” na stránce 2
V dnešní době jste závislí na elektronické poště jako na základním pracovním nástroji. Operační systém i5/OS používá protokoly, jako například SMTP (Simple Message Transfer Protocol) a POP (Post Office Protocol), aby byly vaše e-maily přijímány a odesílány po síti hladce a efektivně.

Související úlohy

“Zaregistrování uživatelů e-mailu” na stránce 18
Abyste mohli zaregistrovat uživatele e-mailu, musíte vytvořit uživatelské profily.

Související odkazy

Create and Send MIME E-mail (QtmsCreateSendEmail) API

Send MIME Mail (QtmmSendMail) API

Nastavení e-mailových klientů POP

Chcete-li přijímat a ukládat e-mail pomocí serveru POP, musíte nejprve nastavit klienta.

Systém používá server POP k ukládání a doručování e-mailu. E-mailový klient pracuje se serverem POP při přijímání a ukládání e-mailu pro uživatele na straně klienta. K dispozici je řada e-mailových klientů, kteří podporují POP, včetně klientů Eudora, Outlook Express a Lotus Notes. Postup při konfigurování klienta je specifický pro rozhraní každého klienta. Informace, které musíte zadat, jsou však stejné. Jestliže používáte například Outlook Express, budete postupovat takto:

1. Shromáždění informací o klientském programu e-mailu POP.

- ID uživatele a plně kvalifikované jméno domény (jméno hostitele a jméno domény). Jedná se o uživatelovu e-mailovou adresu, která slouží k získání pošty a která má obvykle tvar: ID_uživatele@jméno_hostitele.jméno_domény.

  Poznámka: U některých klientů je třeba zadat adresu hostitele několikrát: při určení hostitelského serveru POP pro přijímání pošty, při určení hostitele SMTP pro odesílání pošty a při určení odesílatele pošty pro příjemce.
- Uživatel POP nebo jméno účtu. Je stejné jako jméno profilu uživatele operačního systému i5/OS.
- Heslo uživatele. Toto heslo musí být stejné jako heslo profilu uživatele operačního systému i5/OS.

2. Označení uživatele a uživatelovy preference. Například v aplikaci Outlook Express klepněte na položku **Nástroje → Účty** a potom klepněte na kartu **E-mail**, abyste mohli identifikovat informace o uživateli a o jeho preferencích.
   - Jméno uživatele. Je to jméno profilu uživatele operačního systému i5/OS.
   - E-mailová adresa uživatele. To je ID uživatele a plně kvalifikované jméno domény.
   - Zpáteční adresa. Může být stejná jako e-mailová adresa uživatele, kterou určí administrátor sítě, v systému však musí existovat profil uživatele operačního systému i5/OS.
3. Určení serveru odchozí pošty SMTP. Na e-mailovém klientovi je třeba určit server SMTP, protože to je server, který umožní uživatelům klienta odesílat poštu. Například v aplikaci Outlook Express klepněte na **Nástroje → Účty**, vyberte e-mailový účet a klepněte na tlačítko **Vlastnosti**. Klepněte na kartu **Servery** a identifikujte server SMTP.
   - Uživatel POP nebo jméno účtu. Jedná se o ID uživatele v uživatelově e-mailové adrese. Je to také jméno profilu uživatele operačního systému i5/OS.
   - Server odchozí pošty SMTP. Jedná se o hostitelské jméno systému.
4. Určení serveru příchozí pošty POP. Například v aplikaci Outlook Express klepněte na **Nástroje → Účty**, vyberte e-mailový účet a klepněte na tlačítko **Vlastnosti**. Klepněte na kartu **Servery** a identifikujte server POP.
   - Server příchozí pošty. Jedná se o hostitelské jméno systému.
5. Nakonfigurujte klientský program k používání protokolu TLS/SSL. Například v aplikaci Outlook Express při konfiguraci postupujte následujícím způsobem:
   a. Klepněte na **Nástroje → Účty** a vyberte e-mailový účet.
   b. Klepněte na **Vlastnosti** a potom klepněte na kartu **Servery**.
   c. Vyberte možnost **Server vyžaduje ověření** a klepněte na **Nastavení**.
   d. Vyberte možnost **Použít stejné nastavení jako server příchozí pošty** a klepněte na tlačítko **OK**.
   e. Klepněte na kartu **Upřesnit** a vyberte možnost **Tento server požaduje zabezpečení připojení (SSL)** pro oba poštovní servery, příchozí (POP) a odchozí (SMTP). Klepněte na **OK**.
   f. Klepněte na **Použít** a potom klepnutím na tlačítko **OK** zavřete okno Vlastnosti.

JavaMail

Prostředí JavaMail slouží k vývoji klientských aplikací pro zpracování e-mailu.

Rozhraní JavaMail API poskytuje vývojové prostředí nezávislé na platformě a protokolu. Toto prostředí můžete použít k vytváření klientských aplikací pro e-mail na základě technologie Java. Rozhraní JavaMail API můžete použít při vytváření poštovního klienta, který bude schopen odesílat multimediální poštovní zprávy a který umožní implementaci protokolu IMAP (Internet Mail Access Protocol) podporujícího složky, autentizaci a práci s přílohami.

Vzhledem k tomu, že protokol SMTP podporuje pouze znaková data, využívá toto rozhraní k prezentaci komplexních dat (textových a binárních), jako například formátovaného textu, souborů příloh a multimediálního obsahu MIME (Multipurpose Internet Mail Extensions). Jestliže používáte rozhraní Send MIME Mail (QtmmSendMail) API, musí vaše aplikace převést data do odpovídajícího tvaru. Implementace prostředí JavaMail poskytuje podporu pro integrované zpracování MIME.

Komponenty JavaMail jsou součástí sady IBM Developer Kit for Java.

Související pojmy

JavaMail

Odesílání souborů pro souběžný tisk jako souborů ve formátu PDF

Soubory pro souběžný tisk ve formátu PDF (Adobe Portable Document Format) můžete odesílat a distribuovat pomocí e-mailu.

S použitím licencovaného programu IBM Infoprint Server for iSeries (5722-IP1) můžete z libovolného výstupu z operačního systému i5/OS vytvořit soubory ve formátu Adobe PDF. Tyto soubory PDF lze odesílat jako přílohy e-mailu. Můžete odeslat jednotlivý soubor pro souběžný tisk na danou adresu. Také je možné rozdělit soubor pro souběžný tisk do několika souborů PDF a zaslat každý soubor na jinou adresu. Pomocí této metody můžete posílat faktury zákazníků do samostatných souborů PDF a odesílat příslušné faktury na e-mailové adresy jednotlivých zákazníků. Chcete-li používat tuto metodu výstupu, potřebujete mít nainstalovaný licencovaný program IBM Infoprint Server for iSeries.

Související informace


InfoPrint Server User's Guide PDF


IBM eServer iSeries Printing Redbooks VI -- The Output of e-business

Použití LDAP pro adresy

Můžete použít LDAP (Lightweight Directory Access Protocol) a vytvořit veřejný seznam uložený v distribučním adresáři systému.

Funkce, kterou dříve zajišťovalo rozhraní MAPI, můžete nahradit pomocí produktu IBM Tivoli Directory Server for i5/OS (IBM implementace LDAP). Pomocí LDAP můžete zajistit jednoduchý seznam adres, ke kterému mohou přistupovat z klientské aplikace všichni uživatelé.

Abyste mohli používat LDAP, proveďte následující úkoly:

1. Spusťte server adresářů.
2. Publikujte informace na adresářovém serveru.
3. Nakonfigurujte poštovního klienta na používání LDAP. Kroky nutné pro dokončení tohoto úkolu závisí na vašem poštovním klientu (například Netscape nebo Eudora). Ve vlastnostech poštovního klienta nastavte server LDAP jako adresářový server pro adresování elektronické pošty.

Související úlohy

Začínáme se serverem adresářů

Zveřejnění informací na server adresářů

Související odkazy

IBM Tivoli Directory Server for i5/OS (LDAP)

Odeslání e-mailu pomocí distribučních služeb SNA

E-mail z vašeho systému můžete odeslat pomocí klientského programu SNDAS (Systems Network Architecture distribution services). Odesilatel e-mailu musí být lokální uživatel SNADS.

Nezbytné předpoklady

Lokální uživatel SNADS musí mít takový profil uživatele, aby byl tento uživatel zapsán v položce systémového distribučního adresáře. Pokud chcete zapsat lokální e-mailové uživatele SNADS, přečtěte si téma Zaregistrování uživatelů e-mailu.

Při odesílání e-mailu postupujte následujícím způsobem:

1. Ve znakově orientovaném rozhraní i5/OS zadejte příkaz SNDDST (Odeslání distribuce) a stiskněte klávesu Enter.
2. Stiskněte klávesu F10 a prohlédněte si všechny parametry.

3. Do prvního náznaku *Information to be Sent* zadejte příkaz *LMSG a stiskněte klávesu Enter.
4. Zadejte uživatelské ID příjemce a adresu serveru nebo internetovou adresu.
5. Zadejte popis zprávy do náznaku *Description*.
6. Stiskněte klávesu Page Down a napište svůj e-mail do náznaku *Long Message*.
7. Stisknutím klávesy Enter e-mail odešlete.

Poznámka: Při odesílání e-mailu pomocí příkazu SNDDST (Odeslání distribuce) můžete také použít internetové adresy.

Související úlohy

"Zaregistrování uživatelů e-mailu" na stránce 18
Abyste mohli zaregistrovat uživatele e-mailu, musíte vytvořit uživatelské profily.

"Přijímání e-mailu pomocí distribučních služeb SNA" na stránce 33
E-mail na systému můžete přijímat pomocí klientského programu SNADS (Systems Network Architecture distribution services). Příjemcem pošty musí být lokální uživatel SNADS.

Nastavení záhlaví kvůli rozlišení mezi příjemci

Příkaz HGDSTA (Změna distribučních atributů) změní obsah atributů služby zpráv (podpora X.400) pro distribuci pošty.

Parametr KEEPRCP (Keep Recipient) určuje, které informace o příjemci jsou uloženy a odeslány v rámci každé distribuce pošty. Nastavení tohoto parametru ovlivňuje, jaké se vytvoří záhlaví MIME u poznámky z SNDDST.

Aby se příznaky CC a BCC objevily v záhlaví MIME (a na obrazovkách klientů), musíte nastavit parametr KEEPRCP na hodnotu *ALL. Bez ohledu na nastavení tohoto parametru se příjemci BCC nezobrazí, protože se ani zobrazit nemají. Příjemci TO a CC se zobrazí v textu poznámky SNDDST.

Typy obsahu MIME

Standardní internetové textové poznámky se skládají z obecného záhlaví a textové části. Avšak poznámky MIME mohou obsahovat více částí, které umožňují zahrnout do textu multimediální připojení.

Jestliže obecné záhlaví obsahuje typ obsahu Multipart/Mixed, následuje jedno nebo více připojení. Každé připojení má počáteční a koncový okraj. Identifikátor okraje je nastaven na parametr *boundary*=, který následuje za příznakem záhlaví Content-Type. Příklad poznámky MIME s více částmi najdete na Obrázku 1. U tohoto příkladu má každá část typ obsahu a každý textový typ obsahu může mít definovánu volitelnou znakovou sadu.

```
     From
@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com Wed
Jan 10
11:33:18 1996 Return-Path: <@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com> Received: from SYSNAM6.city.company.com by
fakeps2.city.company.com (COMPANY
          OS/2 SENDMAIL VERSION 1.3.2)/1.0) id AA0329; Wed, 10
Jan 96 11:33:18 -0500 Date: Wed, 10
Jan 96
11:33:18 -0500 Message-Id: <9601101633.AA0329@fakeps2.city.company.com> Received:
  from endmail9 by SYSNAM6.CITY.COMPANY. (IBM i5/OS SMTP V03R02M00) with TCP;
Wed, 10
Jan 1996 10:23:42
+0000. X-Sender: popct08@SYSNAM6.city.ibm.com (Unverified) X-Mailer: Windows
Eudora Pro
Version 2.1.2
Mime-Version:1.0Content-Type:multipart/mixed;boundary="====================_821301929==
  _"
_
To: fake@fakeps2.city.company.com From:
endmail9 <popct08@SYSNAM6.city.company.com> Subject:
eudora attachments
X-Attachments:C:\EUDORA\ARGYLE.BMP;--====================_821301929==_
Content-Type: text/plain; charset=

 "us-ascii" An example of using Eudora to send a text
and bitmap.--====================_821301929==_
Content-Type: application/octet-stream; name="ARGYLE.BMP";
x-mac-type="424D5070"; x-mac-creator="4A565752"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=


"ARGYLE.BMP"
Qk12AgAAAAAAHYAAAAoAAAAIAAAACAAAAABAAQAAAAAAAACAAAAAAAAAAAAAAAAAAAQAAAAAAAA
AAAAgAAAgAAAAICAAIAAAACAAIAAgIAAAICAgADAwMAAAAD/AAD/AAAA//8A/wAAAP8A/wD//wAA
////AE1EREREREZEREREREE1E1EREREERsZEREREETURE1EREREGxsZEREREERNRERE1ERE
REbGxsZEREREE1EREE1ERERsbGxsZERETUREREE1ERGxsbGxsZERNREREREE1EbGxsbGxsZE1E
RERERERE1sbGxsbGxsbUREREREREG1sbGxsbGxtZEREREREREbG1sbGxsbG1sZEREREERERsbG1s
bGxsbWxsZEREREGxsbG1sbGxtbGxsZEREREbGxsbG1sbG1sbGxsZEREREbGxsbG1sbWxsbGxsZE
RGxsbGxsbG1tbGxsbGxsZEbGxsbGxsbG1sbGxsbGxsZEbGxsbGxsbW1sbGxsbGxkREbGxsbGxtbG
1sbGxsbGRERERbGxsbG1sbG1sbGxsZEREREbGxsbWxsbG1sbGxkREREREbGxtbGxsbG1sbGRERERE
REbG1sbGxsbG1sZEREREREREbWxsbGxsbG1kREREREREERNbGxsbGxsbG1EREREREREE1EbGxsbGxs
ZE1EREREREETUREbGxsbGxkRE1EREREERNREREbGxsbGRERE1EREREE1EREREbGxsZEREREE1ERETURE
REREbGxkRERERE1ERNREREREREbGRERERERE1E1EREREREREZEREREREREE3UREREREREREREREREREE--====================_821301929==_--
```

Obrázek 2. Příklad poznámky MIME s více částmi

Podpora internetového adresování pro příkaz SNDDST

Můžete odesílat e-mail na Internet pomocí příkazu SNDDST tak, že zadáte internetovou e-mailovou adresu do náznaku *Internetový Příjemce*.

Používá-li vaše síť SNADS (distribuční služby SNA) a nějakou kancelářskou aplikaci k odesílání a přijímání e-mailů, je třeba, abyste nakonfigurovali poštovní systém tak, aby uživatelé mohli používat internetové adresy s příkazem SNDDST (Odeslání distribucí).

Při konfiguraci poštovního systému postupujte takto:

1. Ve znakově orientovaném rozhraní serveru i5/OS zadejte: ADDDIRE USRID(INTERNET GATEWAY) USRD('Allow SNDDST to send INTERNET Mail') SYSNAME(INTERNET) MSFSRVLVL(*USRIDX) PREFADR(NETUSRID *IBM ATCONTXT)
2. Zadejte CHGDSTA SMTPRTE(INTERNET GATEWAY) a stiskněte klávesu Enter.

Nyní mohou vaši uživatelé SNADS odesílat e-maily na Internet pomocí příkazu SNDDST tak, že zadají internetovou e-mailovou adresu do náznaku *Internetový Příjemce*.

Související informace

AS/400 Electronic-Mail Capabilities Redbook

Připojení souborů

Při odesílání e-mailu pomocí příkazu SNDDST můžete ke zprávě připojit také soubor nebo dokument.

E-mail s připojeným souborem nebo dokumentem můžete odeslat pomocí příkazu SNDDST (Odeslání distribuce). Pomocí příkazu SNDDST je možné poslat v jednom okamžiku pouze jeden dokument nebo soubor. Jestliže byste chtěli odeslat více příloh, odešlete poštu MIME pomocí rozhraní QtmmSendMail API.

Chcete-li k elektronické poště připojit *dokument* ve znakově orientovaném rozhraní, napište:

```
SNDDST TYPE(*DOC) DSTD(váš popis) TOUSRID(jakýkoliv uživatel) DOC(váš dokument) FLR(vaše složka)
```

Chcete-li k elektronické poště připojit *soubor* ve znakově orientovaném rozhraní, napište:

```
SNDDST TYPE(*FILE) DSTD(popis) TOUSRID(jakýkoliv uživatel)
MSG(volitelná zpráva) DOCFILE(vaše knihovna/soubor) DOCMBR(váš člen)
```

Obdržíte-li chybové zprávy, je možné, že se pokoušíte odeslat soubor nebo dokument ve formátu, který není kompatibilní s příkazem SNDDST. Můžete použít CL příkazy i5/OS CPY a převést soubor na soubor nebo dokument, který je kompatibilní s příkazem SNDDST.

Konverze typů souborů pro odeslání pomocí SNDDST

Je-li již vytvořen soubor pro souběžný tisk a existuje-li fyzický soubor a příslušná složka, je zapotřebí konvertovat soubor do formátu, který je možno odeslat.

1. Soubor pro souběžný tisk přemístěte do fyzického souboru databáze:

   ```
   CPYSPLF   FILE(soubor pro souběžný tisk)  TOFILE(databázový soubor)  JOB(úloha3/úloha2/úloha1)
   SPLNBR(číslo souběžného tisku) TOMBR(člen)
   ```

2. Fyzický soubor databáze přemístěte do složky:

   ```
   CPYTOPCD   FROMFILE(knihovna/databázový soubo)  TOFLR(složka) FROMMBR(člen)  REPLACE(*YES)
   ```

3. Odešlete dokument:

   ```
   SNDDST   TYPE(*DOC)  TOUSRID(adresa uživatele) DSTD(MAIL) DOC(člen)  FLR(složka)
   ```

   Související odkazy

   Send MIME Mail (QtmmSendMail) API

Přijímání e-mailu pomocí distribučních služeb SNA

E-mail na systému můžete přijímat pomocí klientského programu SNADS (Systems Network Architecture distribution services). Příjemcem pošty musí být lokální uživatel SNADS.

Chcete-li přijímat e-mail, postupujte následujícím způsobem.

1. Ve znakově orientovaném rozhraní zadejte příkaz QRYDST (Dotaz na distribuci) a stiskněte klávesu F4. Objeví se seznam distribucí.
2. Stiskněte klávesu F10 a prohlédněte si přídavné parametry.
3. Do pole **Soubor pro příjem výstupu** zadejte jména souboru a knihovny, která jsou snadno zapamatovatelná, a stiskněte klávesu Enter. Systém vytvoří fyzické soubory.
4. Napište příkaz WRKF (Práce se soubory) a stiskněte klávesu Enter. Objeví se obrazovka Práce se soubory.
5. Napište jména souboru a knihovny, která jste zadali v kroku 3, a stiskněte klávesu F4.
6. Na obrazovce se objeví seznam všech distribucí (elektronické pošty). Napište číslici 5 vedle distribuce, kterou chcete zobrazit, a stiskněte klávesu Enter.
7. Na obrazovce DSPPFM (Zobrazení členu fyzického souboru) stiskněte klávesu Enter.
8. Na další obrazovce najdete dlouhý řetězec čísel pro každou elektronickou poštu. Zkopírujte sedmý až dvacátý šestý znak.
9. Stiskněte dvakrát klávesu F3 a ukončete práci.
10. Napište příkaz RCVDST (Příjem distribuce) a stiskněte klávesu Enter.
11. Do pole **Identifikátor distribuce** vložte sedmý až dvacátý šestý znak, který jste zkopírovali.
12. Do pole **Soubor pro příjem výstupu** zadejte jméno nového souboru a stejné jméno knihovny, které jste použili již dříve, a stiskněte klávesu Enter.

13. Napište příkaz DSPPFM (Zobrazení členu fyzického souboru), abyste zobrazili soubor, který jste právě vytvořili.
14. Stiskněte klávesu F20 (Shift + F8) a posuňte se doleva, kde si můžete přečíst zprávu nebo zprávy.

Související úlohy

"Odeslání e-mailu pomocí distribučních služeb SNA" na stránce 30
E-mail z vašeho systému můžete odeslat pomocí klientského programu SNDAS (Systems Network Architecture distribution services). Odesilatel e-mailu musí být lokální uživatel SNADS.

Správa e-mailu

Zkušený uživatel nebo administrátor může spravovat servery elektronické pošty, uživatele a zprávy tak, aby byla zajištěna distribuce elektronické pošty v síti.

Kontrola poštovních serverů

Jedním z nejčastějších problémů týkajících se e-mailu je ten, že nejsou spuštěny správné servery. Před použitím poštovních serverů ověřte jejich stav a ujistěte se, že jsou všechny spuštěné.

Chcete-li ověřit stav serverů, postupujte následujícím způsobem:

1. V produktu System i Navigator rozbalte ***systém*** → **Správa činnosti systému** → **Úlohy serveru**.
2. Ověřte, že je aktivní server SMTP. V seznamu Aktivní úlohy serveru ve sloupci Jméno úlohy najděte úlohy **Qtsmtp**.
3. Jestliže zde nejsou uvedeny žádné úlohy **Qtsmtp**, spusťte servery SMTP.
4. Ověřte, že je aktivní funkce MSF (Mail Server Framework). V seznamu Aktivní úlohy serveru ve sloupci Jméno úlohy najděte úlohy **Qmsf**.
5. Jestliže zde nejsou uvedeny žádné úlohy, zadejte ve znakově orientovaném rozhraní příkaz STRMSF (Start the Mail Server Framework).
6. Ověřte, že je aktivní server POP. V seznamu Aktivní úlohy serveru ve sloupci Jméno úlohy najděte úlohy **Qtpop**.
7. Jestliže zde nejsou uvedeny žádné úlohy **Qtpop**, spusťte POP servery.
8. Ověřte, že je aktivní server SNADS. V seznamu Aktivní úlohy serveru ve sloupci Jméno úlohy najděte úlohy **Qsnads**.
9. Jestliže zde nejsou uvedeny žádné úlohy QSNADS, spusťte SNADS. Ve znakově orientovaném rozhraní zadejte příkaz STRSBS QSNADS.

Chcete-li, aby e-mail fungoval správně, musí být spuštěny všechny poštovní servery.

Související pojmy

"Spuštění a zastavení e-mailových serverů" na stránce 19
Spuštěním požadovaných serverů se ujistíte, že vše řádně funguje a že se provedly veškeré zadané změny konfigurace. Někdy bývá nutné servery restartovat. To lze provést tak, že servery zastavíte a potom provedete kroky potřebné pro jejich restartování.

"Určování problémů týkajících se e-mailu" na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Odstranění uživatelů e-mailu POP (Post Office Protocol)

Uživatele e-mailu POP (Post Office Protocol) můžete odstranit pomocí System i Navigator.

Jestliže chcete odstranit uživatele e-mailu z operačního systému, musíte odstranit jeho záznam v systémovém distribučním adresáři následujícím způsobem:

1. Ve znakově orientovaném rozhraní zadejte příkaz WRKDIRE (Práce se záznamy adresáře).
2. Pomocí tabelátoru přejděte na pole *Opt* u uživatele, kterého chcete vymazat.
3. Napište 4 (Odstranit) a stiskněte klávesu Enter. Odstranění potvrďte dalším stisknutím klávesy Enter. Tím zabráníte, aby byla do uživatelovy schránky elektronické pošty POP doručována pošta.

4. Přihlašte se do klientského programu pošty POP jako tento uživatel. Přijměte a vymažte veškerou elektronickou poštu.

Zabránění rozdělování velkých e-mailových zpráv

Pravděpodobně budete potřebovat nastavit určité parametry, aby nedocházelo k rozdělení dlouhých e-mailových zpráv na menší, nečitelné části.

Server SMTP může být nakonfigurován tak, aby rozdělil dlouhé zprávy do menších celků. Mnoho poštovních klientů však neumí tyto části znovu složit, což má za následek vznik nečitelných zpráv. Jestliže zjistíte, že příjemci nemohou číst dlouhé zprávy, protože tyto zprávy jsou rozděleny do několika částí, můžete zablokovat funkci serveru SMTP, která dělí zprávy na menší celky.

Pokud chcete zablokovat dělení zpráv na serveru SMTP, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Dvakrát klepněte myší na **POP**. Objeví se dialog Vlastnosti POP.
3. Klepněte myší na kartu **Konfigurace**.
4. Pro pole **Velikost pro rozdělení zprávy** vyberte hodnotu **Žádné maximum**.

Poznámka: Deaktivace dělení zpráv může způsobit problémy při odesílání dlouhých zpráv elektronickou poštou do sítí, které neumí dlouhé zprávy zpracovat.

Související pojmy

"Odstraňování problémů s e-mailem" na stránce 45
Tyto informace vám pomohou vyřešit případné problémy s e-mailem.

Příjem oznámení o stavu doručení e-mailu

Pokud vaši uživatelé chtějí dostávat oznámení o doručení odeslaných zpráv, musíte povolit funkci oznámení o stavu doručení odeslaných zpráv.

Oznámení o stavu doručení umožní vašemu poštovnímu klientovi obdržet zprávy o stavu při doručení, předání nebo selhání e-mailu. Jestliže chcete klientovi umožnit tento požadavek, musíte povolit oznámení o doručení.

Povolujete pouze oznámení o doručení zpráv pro vaše uživatele. Přejí-li si uživatelé používat funkci oznámení o stavu doručení, musí si nastavit příslušné parametry v poštovním klientovi. Parametry se liší v závislosti na poštovním klientovi.

Jestliže chcete povolit oznámení o stavu doručení, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte myší na stránku Přídavné parametry.
4. Vyberte zaškrtávací políčko **Podpora DSN (Delivery Status Notification)** a zadejte Adresa osoby zodpovědné za oznámení typu DSN.
5. Klepněte na **OK**.

Použití funkce oznámení o stavu doručení aktivuje prostředky, které mohou ovlivnit maximální počet příjemců jednoho e-mailu.

Server Domino a SMTP na stejném serveru

Pokud v témže systému spouštíte servery Domino a SMTP (Simple Mail Transfer Protocol), doporučujeme nakonfigurovat je tak, aby se každý zvlášť vázal na specifickou adresu IP.

Pokud jsou v témže systému servery Domino a SMTP, měli byste každému z nich přiřadit adresu IP. Pošta bude potom odesílána uživatelům serveru Domino nebo SMTP s použitím příslušné adresy IP a přesto, že port je sdílený, bude pošta zpracovávána pouze serverem, pro který je určena.

Chcete-li zajistit, aby server SMTP použil specifickou internetovou adresu, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
3. Klepněte myší na kartu **Vazby**.
4. Vyberte přepínač **Použít všechna rozhraní** k připojení všech rozhraní k portu 25.
5. Použijte přepínač **Vybrat rozhraní** k výběru rozhraní, která chcete použít k propojení serveru a klienta.

   Poznámka: Pokud chcete použít funkci NAT (network address translation) buď v systému, nebo na bráně firewall musíte nastavit klienta SMTP operačního systému i5/OS tak, aby používal jednu konkrétní internetovou adresu.
6. Klepněte na **OK**.

Nyní server SMTP přijme pouze poštu, která je adresována na tuto internetovou adresu. Zkontrolujte server DNS (Domain Name System), lokální hostitelskou tabulku a systémový distribuční adresář a ujistěte se, že obsahují tuto vynucenou internetovou adresu.

Informace o svázání serveru Domino SMTP se specifickou adresou protokolu TCP/IP najdete na webu Lotus Domino Reference Library.

Související pojmy

"Plánování e-mailu" na stránce 9
Před nastavením e-mailu byste měli mít základní představu o tom, jakým způsobem jej budete na systému používat.

Filtrování IP a NAT

Domino LDAP a Directory Server ve stejném systému

Pokud používáte Domino LDAP a IBM Tivoli Directory Server for i5/OS (Directory Server) ve stejném systému, doporučujeme vám nakonfigurovat tyto aplikace tak, aby se každá zvlášť vázala na specifickou IP adresu.

Pokud jsou servery Domino LDAP a Directory Server hostovány ve stejném systému, můžete pro ně buď nastavit odlišná čísla portů, nebo každý z nich vázat na určitou IP adresu. Změna čísla portu může mít negativní následky pro klienty, takže nejlepším řešením bude přiřazení specifické IP adresy každému serveru. Domino a SMTP budou používat pro adresování e-mailu příslušný server LDAP.

Chcete-li zajistit, aby server Directory Server použil specifickou internetovou adresu, postupujte takto:

1. V produktu System i Navigator vyberte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
2. Klepněte pravým tlačítkem myši na **Adresář** a vyberte **Vlastnosti**.
3. Klepněte myší na kartu **Síť**.
4. Klepněte na volbu **IP adresy**.
5. Vyberte volbu **Použít vybrané IP adresy** a ze seznamu zadejte, které rozhraní chcete přiřadit.
6. Klepněte myší na **OK** a uzavřete stránku Adresář - IP adresy.
7. Klepněte myší na **OK** a uzavřete stránku Vlastnosti adresáře.
8. Volitelné: Používáte-li server Domino LDAP, prohlédněte si Lotus Domino Reference Library. Zde najdete návod, jak serveru Domino LDAP přiřadit určitou adresu TCP/IP.
9. Spusťte servery pro e-mail.

Související informace

Lotus Domino Reference Library

Správa výkonu serveru SMPT (Simple Mail Transfer Protocol)

Zde jsou uvedeny tipy pro správu přetíženého serveru SMTP, který používá paralelní zpracování.

Server SMTP může být přetížený tím, že využívá veškerou kapacitu na přidání a ukončení předspuštěných úloh pro každý požadavek elektronické pošty.

Pokud zjistíte, že počet předspuštěných úloh ovlivňuje výkon systému, můžete nastavit nižší prahovou hodnotu. Chcete-li více úloh, můžete nastavit počet předspuštěných úloh na vyšší hodnotu.

S nastavenými předspuštěnými úlohami běží každý požadavek elektronické pošty jako jeho vlastní úloha. Tento způsob zpracování umožňuje, aby se každá úloha zaměřila pouze na svého klienta nebo na potřeby a požadavky programů serveru. Každá úloha může provádět volání s delší časovou prodlevou, aby umožnila zapsání hostitelských jmen, a zabránila tak příjmu nevyžádaných hromadných poštovních zpráv.

V rámci správy zatíženého serveru SMTP můžete změnit tyto hodnoty:

- Počet úloh, které se mají spustit při inicializaci.
- Prahový počet úloh.
- Počet úloh, které se mají přidat, když systém dosáhne prahové hodnoty.
- Maximální počet spuštěných úloh.
- Výběr podsystému pro úlohy.

Abyste mohli spravovat zatížený systém, musíte změnit hodnoty na serveru SMTP a u klienta SMTP.

Server SMTP pracuje s démonem a předspuštěnými úlohami: QTSMTPSRVD a QTMSMTPSRVP. Klient SMTP pracuje s démonem a předspuštěnými úlohami: QTSMTPCLTD a QTSMTPCLTP.

Jestliže chcete změnit hodnoty na serveru SMTP, postupujte takto:

1. Ve znakově orientovaném rozhraní zadejte příkaz CHGPJE (Změna záznamů úlohy).
2. Zadejte do náznaku následující hodnoty a stiskněte klávesu Enter.

Náznak	**Hodnota**
Podsystém	QSYSWRK
Knihovna	QSYS
Program	QTMSSRCP
Knihovna	QTCP
Spustit úlohy	*SAME
Počáteční počet úloh	4
Prahová hodnota	2
Dodatečný počet úloh	2
Maximální počet úloh	20

Tyto hodnoty zaručují, že systém spustí čtyři předspuštěné úlohy, a jakmile dostupných úloh klesne pod dvě, spustí dvě dodatečné úlohy. Současně povolí nejvýše dvacet předspuštěných úloh.

Změna hodnot pro server SMTP

Chcete-li změnit hodnoty pro server SMTP, použijte tuto proceduru.

1. Ve znakově orientovaném rozhraní zadejte příkaz CHGPJE (Změna záznamů úlohy).

2. Zadejte do náznaku následující hodnoty a stiskněte klávesu Enter.

Náznak	Hodnota
Podsystém	QSYSWRK
Knihovna	QSYS
Program	QTMSSRCP
Knihovna	QTCP
Spustit úlohy	*SAME
Počáteční počet úloh	4
Prahová hodnota	2
Dodatečný počet úloh	2
Maximální počet úloh	20

Tyto hodnoty zaručují, že systém spustí čtyři předspuštěné úlohy, a jakmile dostupných úloh klesne pod dvě, spustí dvě dodatečné úlohy. Současně povolí nejvýše dvacet předspuštěných úloh.

Změna hodnot pro klienta SMTP

Chcete-li změnit hodnoty pro klienta SMTP, použijte tuto proceduru.

1. Ve znakově orientovaném rozhraní zadejte příkaz CHGPIE (Změna záznamů úlohy).
2. Zadejte do náznaku následující hodnoty a stiskněte klávesu Enter.

Náznak	Hodnota
Podsystém	QSYSWRK
Knihovna	QSYS
Program	QTMSCLCP
Knihovna	QTCP
Spustit úlohy	*SAME
Počáteční počet úloh	4
Prahová hodnota	2
Dodatečný počet úloh	2
Maximální počet úloh	20

Tyto hodnoty zaručují, že klient SMTP spustí čtyři předspuštěné úlohy, a jakmile počet dostupných úloh klesne pod dvě, spustí dvě dodatečné úlohy. Současně povolí nejvýše dvacet předspuštěných úloh.

Výběr nového subsystému pro úlohy serveru SMTP

Pomocí uvedeného postupu můžete vybrat nový subsystém pro úlohy serveru SMTP (Simple Mail Transfer Protocol).

1. Pro server SMTP můžete zadat samostatný subsystém. Tím by se měl zvýšit výkon, protože se vyloučí potřeba sdílet prostředky.
2. Jestliže chcete zadat samostatný subsystém, postupujte takto:
   a. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
   b. Klepněte pravým tlačítkem myši na **SMTP** a vyberte **Vlastnosti**.
   c. Klepněte myší na kartu **Přídavné parametry**.
   d. Vyberte přepínač **Popis subsystému**.
   e. Zadejte nové jméno subsystému a knihovnu, kde bude vytvořen popis subsystému a fronta úloh.

Program zkontroluje, zda existuje zadaný subsystém. Pokud neexistuje, program ho vytvoří společně s položkami směrovací tabulky, položkami automatického spuštění úloh, položkami předspuštěných úloh a popisy úloh. I když subsystém ještě neexistuje, knihovna pro popis subsystému a frontu úloh již musí existovat. Při zpracování startovací úlohy tato úloha nastaví parametry pro nově vytvářený subsystém a pak předá úlohy pro dávkové spuštění serveru tomuto subsystému.

Referenční informace k elektronické poště

Zde můžete najít referenční informace o záznamech v žurnálu poštovního serveru, příkazech protokolu SMTP (Simple Mail Transfer Protocol) a klíčových slovech a parametrech protokolu POP (Post Office Protocol).

Položky žurnálu poštovního serveru

K pochopení kódů a zpráv v žurnálu použijte následující informace.

Následující tabulky obsahují podrobnější informace o čtení položek žurnálu.

- "Zkratky položek žurnálu"
- "Záznamy v protokolu pro klienta SMTP" na stránce 40
- "Protokolování položek pro server SMTP" na stránce 41
- "Protokolování položek pro server Bridge" na stránce 41
- "Služba MSF (Message Switching Facility) při ukončení vytváří funkce" na stránce 42

Zkratky položek žurnálu

Zkratka	Definice
LIN	Local in, poznámka přijatá při lokálním doručení. Následuje IP adresa, odkud byla odeslána poznámka.
RIN	Relay in, poznámka přijatá při přenosu na jiný přenosový démon SMTP. IP adresa, kterou poslal následuje.
R	Příjemce (Recipient)
O	Původce (Originator)
U	Neznámý příjemce (Undelivered recipient)
QTMSINQ	Vstupní fronta SMTP
QTMSOUTQ	Výstupní fronta SMTP
QTMSBSSQ	Zádržná fronta (Holding queue). Sem se ukládají zprávy, je-li překročen práh paměti systému.
QTMSRTQ1	Fronta pro opakování první úrovně (First level retry queue)
QTMSRTQ2	Fronta pro opakování druhé úrovně (Second level retry queue)
RRSL	Rozlišený příjemce (Recipient resolved)

Každé položce žurnálu předchází dvouznakový podtyp nebo kód. První znak podtypu nebo kódu obsahuje identifikátor funkce pro položku. Druhý znak podtypu nebo kódu obsahuje operaci, kterou tato položka žurnálu dokumentuje. Identifikátory funkce jsou uvedeny v následující tabulce.

Identifikátor funkce	Popis
7	Položka serveru Bridge.
8	Klient SMTP.
9	Server SMTP.
A	Nedoručení MSF.

Identifikátor funkce	Popis
B	Lokální doručení MSF.
C	Předání zprávy MSF.
D	Vytvoření zprávy POP.
E	Rozhraní SendMail API
F	Domino MTA
G	Posílání programu typu snap-in tunelem.
H	SNADS (přepínač).
I	Kontrolující program MIME (program typu snap-in pro lokální doručení).
L	FAX (lokální doručení).
M	SNADS.
O	Filtrování.
P	Ukončení MSF SMTP pro rozpoznání adresy.

Všechny zde zdokumentované položky žurnálu používají typ záznam v protokolu (LG).

Záznamy v protokolu pro klienta SMTP

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Odstranění zásobníku z fronty pro zpracování.	8B	Ihned po nastavení jistícího příznaku zapsat do protokolu odstranění zprávy z fronty.
LG	Úspěšné doručení pošty.	88 82	Zapsat úspěšné odeslání pošty. Zapsat každého příjemce.
LG	Nedoručitelná pošta.	83	Zapsat nedoručitelnou poštu.
LG	Časová prodleva 1. úrovně.	8C	Zapsat do protokolu při přidání do opakovaného pokusu o zavedení do fronty 1. úrovně.
LG	Časová prodleva 2. úrovně.	8D	Zapsat do protokolu při přidání do opakovaného pokusu o zavedení do fronty 2. úrovně.
LG	Pošta je připravena na nový pokus.	8E 8F	Zapsat do protokolu, když se opakovaná pošta vrátí zpět do QTMSOUTQ.
LG	COD odesílán zpět odesílateli.	87	Zapsat do protokolu, když potvrzení při doručení (COD) je zařazeno do fronty BRSR.
LG	Zpracování není možné, prostředek je zaneprázdněný.	86	Zapsat do protokolu, když se pošta vrátí zpět do QTMSOUTQ, jelikož matice spojení je plná.
LG	Prozkoumat záznamy příjemce.	86	Zapsat do protokolu, když se pošta vrátí zpět do QTMSOUTQ, jelikož se změnil stav příjemce, tj. záznam MS je připraven doručit zprávu.

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Nedoručitelné.	87	Zapsat do protokolu přenos pošty do QTMSINQ kvůli zprávě o nedoručení, dvě místa.
LG	Dotaz MX.	8K	Zapsat do protokolu selhání res_send a errno udávající proč, pokud se nezdaří současně s dotazem vyrovnávací paměti.

Protokolování položek pro server SMTP

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Obdržení pošty.	94 91 92 9T 99	Zapsat do protokolu obdržení pošty ihned po získání koncové sekvence CRLF <.> CRLF (lokální). Odesílatel zprávy a příjemce jsou zapsáni do protokolu. Velikost zprávy *nnnnn*, kde *nnnnn* je počet bajtů. MSGID
LG	Obdržení přenesené pošty.	95 91 92	Zapsat MAIL do protokolu ihned po získání koncové sekvence CRLF <.> CRLF (přeneseno). Odesílatel zprávy a příjemce jsou zapsáni do protokolu.
LG	Předání pošty na server Bridge.	97	Zapsat do protokolu položku MAIL do QTMSINQ (příchozí pošta).
LG	Předání pošty klientovi pro vzdálené doručení.	96	Zapsat do protokolu položku MAIL do QTMSOUTQ (přenesená pošta).
LG	SPOJENÍ ODMÍTNUTO 1.2.3.4....	9S	Zapsat do protokolu spojení odmítnutá na základě vyhrazených nastavení spojení. 1.2.3.4 je zamítnutá IP adresa.
LG	ODMÍTNUTÝ PŘENOS 1.2.3.4....	9V	Zapsat do protokolu přenosy odmítnuté na základě vyhrazených nastavení přenosu. 1.2.3.4 je zamítnutá IP adresa.
LG	Odmítnuto serverem SMTP.	9W	Zpráva byla odmítnuta serverem SMTP.

Protokolování položek pro server Bridge

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Vyzvednutí pošty z fronty IN.	7A	Zapsat do protokolu poštu vyřazenou z fronty QTMSINQ.
LG	Předání pošty do SNADS.	7O	Zaznamenat úspěšný přenos do QSNADS.

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Umístění kontejneru do fronty BUSY kvůli využití místa	7L	Zaznamenat, když je pošta ve frontě v QTMSBSSQ kvůli překročení prahové hodnoty.
LG	Vyzvednutí pošty z fronty BUSY.	7M	Zaznamenat vyzvednutí pošty z fronty z QTMSBSSQ. Místo bylo získáno zpět a pošta může být nyní zpracována.
LG	Předání zprávy do MSF.	7H 71 72	Zaznamenat, když je do frameworku vložena zpráva.
LG	Tvorba zprávy COD.	7R 7G	Zaznamenat, když je zpráva COD vložena do frameworku. Zapsat do protokolu MSF MSGID, když se vytváří nová zpráva COD.
LG	Tuto poštu nelze doručit příjemci.	7P 7G	Zaznamenat do protokolu, že jste vytvářeli nedoručitelné upozornění. Zaznamenat do protokolu MSGID nového nedoručitelného upozornění zprávy.

Služba MSF (Message Switching Facility) při ukončení vytváří funkce

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Vytvoření zprávy o nedoručení.	AP A1 A2	Zaznamenat, že nedoručitelná zpráva byla vložena do MSF.
LG	Pošta je doručena do schránky elektronické pošty POP.	B8 B2	Zaznamenat doručení zprávy do lokální schránky pošty POP. IP adresa bude adresářem schránky pošty POP. Příjemce bude také zaznamenán.
LG	Poslání zprávy COD do MSF.	BR B1 B2	Zaznamenat vložení zprávy COD do MSF.
LG	Kontrola dostupnosti.	CN	Zpráva SMTP předávající ukončení MSF. Zaznamenat MSGID, které bylo vloženo zpět do fronty QMSF kvůli nespuštění SMTP.
LG	Zařazení pošty do fronty.	C6 C1 C2	Zapsat do protokolu poštu zařazenou do fronty QTMSOUTQ.
LG	Použití rozhraní Sendmail API.	EH E1 E2 ET	Zaznamenat vytvoření zprávy pomocí rozhraní API SendMail. Velikost zprávy *nnnnn*, kde *nnnnn* je velikost zprávy (všechny přílohy).
LG	Pošta má cíl ve vzdáleném systému připojeném přes SNADS.	G8 G2	Zaznamenat, když je zpráva tunelována. Zahrnout odelání pošty příjemci systémem.

Typ	Akce	Podtypy nebo kódy	Komentář
LG	Přijetí pošty posílané tunelem přes SNADS.	GQ G2	Zaznamenat přijímání zprávy posílané tunelem pro lokální doručení příjemci.
LG	Rozlišení adresy SNADS přepíná z/do.	H1	SNADS předalo zprávu do MSF.
LG	Opětovné vložení analyzované zprávy MIME do rámce.	IH I1 I2 IG	Zapsat do protokolu, když je analyzovaná zpráva MIME opět vložena do MSF.
LG	Zamítnuto filtrování.	OW	Zpráva byla odmítnuta. Je zaznamenáno, zda byla vyřazena nebo uložena. Je zaznamenáno, zda byla přepsána nebo doručena.
LG	Zapsáno programem výstupního bodu SMTP Address Resolution MSF.	P2	Zpráva byla označena takto: • **POP LclDel:** Označena pro program výstupního bodu lokálního doručení POP, aby ji doručil. • **SMTP MsgFwd:** Označena pro předání do SMTP, odkud bude odeslána. • **SMTP NonDel:** Označena kvůli poznámce o nedoručení. • **Parse:** Odeslána do programu kontrolujícího kód. • **PutBk:** Uložena zpět do rámce pro jiné ukončení (např. Domino nebo SNADS). • **chg to SNADS:** Změněn typ adresy na SNADS.

Související úlohy

“Kontrola žurnálů komponent” na stránce 47
Kontrolou žurnálů, které zaznamenávají chyby, můžete určit, jak vyřešit určitý problém s e-mailem.

SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol) je protokol protokolu TCP/IP používaný k odesílání a přijímání elektronické pošty. Obvykle se spolu s protokolem POP3 nebo IMAP (Internet Message Access Protocol) používá k uložení zpráv do schránky elektronické pošty na serveru a k jejich pravidelnému stahování ze serveru pro uživatele.

Příkazy SMTP

Následující tabulka popisuje příkazy SMTP, funkce příkazů a zda je příkaz podporování systémem i5/OS.

Příkaz SMTP	Jeho funkce	Podporována systémem System i
AUTH (Ověření)	Označuje ověřovací mechanismus serveru SMTP. Je podporováno jak PLAIN tak LOGIN.	Ano

Příkaz SMTP	Jeho funkce	Podporována systémem System i
DATA (Data)	Považuje řádky následující za příkazem za zprávu elektronické pošty od odesilatele.	Ano
EHLO (rozšířené Hello)	Povolí rozšíření protokolu SMTP.	Ano
EXPN (Rozbalit)	Požádá příjemce, aby potvrdil, že poštovní seznam byl identifikován.	Ne
HELO (Hello)	Identifikuje odesílatele SMTP pro příjemce SMTP.	Ano
HELP (Nápověda)	Požádá příjemce, aby poslal odesílateli pomocné informace.	Ano
MAIL (Pošta)	Spustí transakci elektronické pošty a doručí elektronickou poštu jednomu nebo více příjemcům.	Ano
NOOP (Žádná operace)	Požádá příjemce, aby odeslal platnou odpověď (ale nezadával žádnou jinou operaci).	Ano
QUIT (Odchod)	Požádá příjemce, aby poslal platnou odpověď a potom uzavřel přenosový kanál.	Ano
RCPT (Příjemce)	Identifikuje jednotlivého příjemce elektronické pošty.	Ano
RSET (Obnovit)	Ukončí aktuální transakci elektronické pošty.	Ano
SAML (Odeslat a odeslat poštou)	Doručí elektronickou poštu jedné nebo více pracovním stanicím nebo příjemcům v případě, že uživatel není aktivní.	Ne
SEND (Odeslat)	Doručí elektronickou poštu jedné nebo více pracovním stanicím.	Ne
SOML (Odeslat nebo odeslat poštou)	Doručí elektronickou poštu jedné nebo více pracovním stanicím nebo příjemcům v případě, že uživatel není aktivní.	Ne
STARTTLS (Spustit zabezpečení transportní vrstvy)	Požádá server SMTP o spuštění vyjednání SSL nebo TLS s klientem SMTP za účelem zřízení relace SSL nebo TLS.	Ano
TURN (Otočit)	Požádá příjemce, aby odeslal platnou odpověď a potom se stal odesilatelem SMTP, nebo požádá příjemce, aby odeslal odmítavou odpověď a zůstal příjemcem SMTP.	Ne
VRFY (Ověřit)	Požádá příjemce, aby potvrdil, že uživatel byl identifikován.	Ano

Související pojmy

“Scénář: Lokální odeslání a přijetí e-mailu” na stránce 4
Tento příklad ukazuje proces zpracování pošty mezi lokálními uživateli.

Protokol POP (Post Office Protocol)

Poštovní rozhraní POP (Post Office Protocol) verze 3 je definováno v dokumentech RFC (Request for Comments) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism) a RFC 2595 (Using TLS with IMAP, POP3, and ACAP). Dokumenty RFC slouží k definování vyvíjejících se internetových standardů.

Klientské programové vybavení používá při komunikaci se serverem POP příkazy nazývané *verb*. Server s protokolem POP i5/OS podporuje tyto příkazy verb.

Příkaz verb a parametry	**Popis**
USER <id>	Předat uživatelské ID.
PASS <heslo>	Heslo.
STAT	Dotaz na schránku elektronické pošty.
LIST <volitelné číslo zprávy>	Statistika dotazů na zprávu.
RETR <číslo zprávy>	Načíst zprávu.
DELE <číslo zprávy>	Vymazat zprávu.
RSET	Resetovat stav vymazání zprávy.
TOP <číslo zprávy> <počet řádek>	Načíst záhlaví zprávy a data.
UIDL <volitelné číslo zprávy>	Získat seznam jedinečných ID zpráv.
NOOP	Žádná operace.
QUIT	Odchod z relace klienta.
CAPA	Vypsat možnosti.
STLS	Spustit zabezpečení transportní vrstvy.

Související pojmy

"Scénář: Lokální odeslání a přijetí e-mailu" na stránce 4
Tento příklad ukazuje proces zpracování pošty mezi lokálními uživateli.

"Protokol POP v operačním systému i5/OS" na stránce 4
Server POP (Post Office Protocol) je e-mailové rozhraní implementované v operačním systému i5/OS. Jedná se o Post Office Protocol verze 3.

Odstraňování problémů s e-mailem

Tyto informace vám pomohou vyřešit případné problémy s e-mailem.

Související úlohy

"Zabránění rozdělování velkých e-mailových zpráv" na stránce 35
Pravděpodobně budete potřebovat nastavit určité parametry, aby nedocházelo k rozdělení dlouhých e-mailových zpráv na menší, nečitelné části.

Určování problémů týkajících se e-mailu

Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Chcete-li určit pravděpodobné problémy s protokolem SMTP, postupujte takto:

1. Ověřte, že je pro e-mail nakonfigurován protokol TCP/IP.
   a. Zkontrolujte, zda jsou nainstalována všechna požadovaná PTF.
   b. Zkontrolujte e-mailové servery a ujistěte se, že jsou potřebné servery spuštěny a že fungují.
2. Ověřte jméno lokální domény.
   a. V produktu System i Navigator rozbalte ***systém*** → **Síť**.
   b. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Vlastnosti**.
   c. Klepněte myší na kartu **Informace o hostitelské doméně** a ověřte jméno místní domény.
3. Nastavte nižší hodnoty SMTP pro opakování.
   a. V produktu System i Navigator rozbalte ***systém*** → **Síť** → **Servery** → **TCP/IP**.
   b. Dvakrát klepněte myší na **SMTP**.

c. Klepněte myší na kartu **Opakované pokusy pro odchozí poštu**.

4. Ověřte, že se uživatelské ID a adresa příjemce nacházejí v systémovém distribučním adresáři.
   a. V produktu System i Navigator rozbalte ***systém*** **→ Uživatelé a skupiny → Všichni uživatelé**.
   b. Klepněte pravým tlačítkem myši na **Profil** uživatelského ID a vyberte **Vlastnosti**.
   c. Klepněte myší na **Osobní** a přejděte na kartu **Pošta**, kde ověříte adresu.
5. Ověřte, zda je položka hostitelské tabulky nezbytná k tomu, aby e-mail dorazil na adresu místa určení.
   a. Ve znakově orientovaném rozhraní napište příkaz CHGTCPHTE (Změna TCP/IP položky tabulky hostitele) a zadejte internetovou adresu e-mailového serveru.
   b. Pokud se neobjeví žádná položka hostitelské tabulky, zadejte hostitelské jméno pro tuto internetovou adresu.
6. Ujistěte se, že jste nepřekročili práh paměti.
   a. V produktu System i Navigator rozbalte ***systém*** **→ Konfigurace a služba → Hardware → Diskové jednotky → Fondy disků**.
   b. Klepněte pravým tlačítkem myši na společnou oblast zdrojového disku, kterou si chcete prohlédnout, a vyberte **Vlastnosti**.
   c. Vyberte kartu **Kapacita**.

   Pokud je využití systému větší než stanoví práh, pošta může přestat fungovat.
7. Ověřte, že je zakázáno dělení e-mailu.
   a. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
   b. Dvakrát klepněte myší na **POP**. Objeví se dialog Vlastnosti POP.
   c. Klepněte myší na kartu **Konfigurace**.
   d. U pole **Velikost pro rozdělení zprávy** ověřte, že je vybrána hodnota **Žádné maximum**.
8. Spusťte příkaz Trasování aplikace TCP/IP. Ve znakově orientovaném rozhraní zadejte TRCTCPAPP.
9. Zkontrolujte žurnály komponent a najděte problém.

Související pojmy

“Řízení přístupu k e-mailu” na stránce 10
Měli byste řídit, kdo přistupuje k systému prostřednictvím e-mailu. Tím ochráníte svá data před svévolnými útoky.

Příklad nezávislých fondů disků

“Řízení přístupu pomocí protokolu POP” na stránce 10
Chcete-li zabezpečit systém, musíte řídit přístup prostřednictvím protokolu POP.

“Odstraňování problémů s rozhraním QtmmSendMail API” na stránce 48
Tento postup vám pomůže při odstraňování problémů s rozhraním Send MIME Mail (QtmmSendMail) API.

Související úlohy

“Kontrola poštovních serverů” na stránce 34
Jedním z nejčastějších problémů týkajících se e-mailu je ten, že nejsou spuštěny správné servery. Před použitím poštovních serverů ověřte jejich stav a ujistěte se, že jsou všechny spuštěné.

“Konfigurování TCP/IP pro e-mail” na stránce 14
Předtím než nakonfigurujete e-mail ve vašem systému, musíte nastavit TCP/IP.

“Kontrola úloh frameworku poštovního serveru” na stránce 48
Měli byste kontrolovat úlohy frameworku poštovního serveru v systému QSYSWRK, abyste byli schopni určit možnou příčinu chyby v rozhraní API QtmmSendMail.

“Kontrola žurnálů komponent” na stránce 47
Kontrolou žurnálů, které zaznamenávají chyby, můžete určit, jak vyřešit určitý problém s e-mailem.

“Hledání příčin nedoručení e-mailu” na stránce 47
Při hledání problémů s nedoručeným e-mailem můžete použít generické ID uživatele. Tato metoda může být užitečná jak při problémech s doručováním e-mailu, tak při problémech s konfigurací.

Související informace

Podpora IBM System i

Kontrola žurnálů komponent

Kontrolou žurnálů, které zaznamenávají chyby, můžete určit, jak vyřešit určitý problém s e-mailem.

Operační systém používá různé fronty, programy a dokumenty žurnálů, které vám pomohou při zjišťování příčin, proč poštovní server nedoručil e-mailovou zprávu. Funkce žurnálování může pomoci odhalit příčiny neúspěchu tím, že nabízí přehled o chybách funkcí systému e-mailu. Žurnálování využívá cykly základní jednotky, takže počítač má nejlepší výkon, když je žurnálování vypnuté.

Funkce žurnálování dokumentuje tyto položky:

- Přechody - programy do fronty, fronty do programu.
- Události - příchod pošty přes server, doručení pošty přes klienta, uložení pošty do opakované fronty nebo do fronty zaneprázdněného prostředku.
- Sledování a některé naměřené údaje - ID zprávy 822, ID zprávy MSF, velikost zprávy, odesílatel, příjemci.

Položky žurnálů jsou uloženy v žurnálových zásobnících. Tyto zásobníky jsou spravovány uživatelem. Když je žurnál plný, zadejte příkaz CHGJRN (Změna žurnálu) a použijte nový žurnálový zásobník. Nová funkce žurnálování SMTP používá žurnál QZMF.

Jestliže chcete žurnálování aktivovat a prohlížet si obsah žurnálů, postupujte takto:

1. V produktu System i Navigator rozbalte ***systém*** **→ Síť → Servery → TCP/IP**.
2. Dvakrát klepněte myší na **SMTP**.
3. Klepněte myší na kartu **Obecné**.
4. Vyberte zaškrtávací políčko **Umožnit zápis záznamů do žurnálu**.
5. Otevřete relaci emulace.
6. Jestliže chcete konvertovat položky žurnálu SMTP do čitelné formy, napište ve znakově orientovaném rozhraní: DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(*jrnlib/zmfstuff*) OUTMBR(*MAR2*) ENTDTALEN(512), kde *jrnlib* je jméno knihovny a *zmfstuff* jméno fyzického souboru.
7. Chcete-li zobrazit položky žurnálu SMTP, zadejte na příkazovém řádku příkaz: DSPPFM FILE(*jrnlib/zmfstuff*) MBR(*MAR2*).
8. Stiskněte klávesu F20 (Shift + F8) a prohlédněte si informace v žurnálu.

Související pojmy

“Určování problémů týkajících se e-mailu” na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Související odkazy

“Položky žurnálu poštovního serveru” na stránce 39
K pochopení kódů a zpráv v žurnálu použijte následující informace.

Hledání příčin nedoručení e-mailu

Při hledání problémů s nedoručeným e-mailem můžete použít generické ID uživatele. Tato metoda může být užitečná jak při problémech s doručováním e-mailu, tak při problémech s konfigurací.

1. Vyberte nebo vytvořte uživatelské ID, pomocí kterého budete dostávat upozornění. Ve znakově orientovaném rozhraní zadejte příkaz CRTUSRPRF (Vytvoření uživatelského profilu) a stiskněte klávesu Enter.
2. Zadejte příkaz WRKDIRE (Práce se záznamy adresáře) a stiskněte klávesu Enter.
3. Zadejte 1 a přidejte tak uživatele do systémového distribučního adresáře.
4. Ujistěte se, že hodnota Mail Store je 2 a hodnota Preferred Address je 3.
5. Stiskněte F19 (Přidání jména pro SMTP).
6. Jako adresu SMTP pro libovolného uživatele POP zadejte NONDELIVERY@lokálníhostitelskýserver.doména.

Tento uživatel obdrží kopii upozornění o nedoručitelné poště.

Poznámka: Zadané ID uživatele musí být skutečným ID, aby mohlo účinně monitorovat upozornění o nedoručení. Odesílatel obdrží kopii upozornění o nedoručení se seznamem příjemců, kteří e-mail nedostali.

Související pojmy

"Určování problémů týkajících se e-mailu" na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Odstraňování problémů s rozhraním QtmmSendMail API

Tento postup vám pomůže při odstraňování problémů s rozhraním Send MIME Mail (QtmmSendMail) API.

Rozhraní QtmmSendMail API může vracet chyby. Popis chybových zpráv vrácených tímto rozhraním najdete v tématu Rozhraní QtmmSendMail API.

Související pojmy

"Určování problémů týkajících se e-mailu" na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Související odkazy

Send MIME Mail (QtmmSendMail) API

Kontrola volání rozhraní API

Chcete-li provést obnovu z chyby rozhraní QtmmSendMail API, ujistěte se, že na obrazovku pracovní stanice dostáváte chybové zprávy z rozhraní API.

Pokud naprogramujete vrácení chyby, program ji vrátí zpět programu. Když však nastavíte tuto hodnotu na 0, jak ukazují následující příklady, chyba se objeví na obrazovce vaší pracovní stanice.

Příklad v jazyce C

```
Qus_EC_t         Snd_Error_Code;
Snd_Error_Code.Bytes_Provided=0;
```

Příklad v jazyce RPG

```
DAPIError     DS
D APIBytes          1     4B 0
D CPFId             9    15
C              Eval    APIBytes   = 0
```

Kontrola souboru MIME

Soubor MIME může způsobovat to, že rozhraní QtmmSendMail API vrátí chybu. Zkontrolujte soubor MIME a odstraňte tyto problémy.

1. Zkontrolujte umístění souboru MIME. Soubor MIME musí být v systému ROOT, musí začínat /, například /myfile.txt, a jméno souboru musí obsahovat cestu /mydirectory/myfile.mime.
2. Zkontrolujte úrovně oprávnění. Profily QMSF a QTCP musí mít oprávnění ke čtení a mazání souboru MIME.
   a. Ve znakově orientovaném rozhraní zadejte příkaz WRKLNK (Práce se spojováním objektů).
   b. Zadejte volbu 9 (Zobrazit), abyste mohli pracovat s oprávněními QMST a QTCP. Objeví se obrazovka Práce s oprávněním.
3. Ujistěte se, že soubor MIME má mezi záhlavím a textem příkaz pro ukončení záhlaví (CRLFCRLF).
4. Ujistěte se, že soubor MIME vyhovuje konvencím RFC pro MIME.

Poznámka: Chcete-li získat další informace o příkazu pro ukončení záhlaví, prohlédněte si oddíl 2.1 v RFC2822 (http://rfc.net/rfc2822.html).

Kontrola úloh frameworku poštovního serveru

Měli byste kontrolovat úlohy frameworku poštovního serveru v systému QSYSWRK, abyste byli schopni určit možnou příčinu chyby v rozhraní API QtmmSendMail.

1. Jestliže MSF přestal zpracovávat zprávu, zkontrolujte chybové zprávy úloh MSF.

2. Po skončení úloh frameworku by měl být soubor MIME vymazán. To znamená, že framework zpracoval soubor MIME. Problém tedy nesouvisí s rozhraním API, ale s konfigurací SMTP.

Související pojmy

“Určování problémů týkajících se e-mailu” na stránce 45
Pomocí těchto jednoduchých kroků můžete určit příčinu problémů s e-mailem.

Informace související s e-mailem

Produktové manuály, publikace IBM Redbooks, webové stránky a další informace v kolekcích témat aplikace Informační centrum, které se vztahují ke sbírce témat E-mail. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Příručky

AnyMail/400 Mail Server Framework Support (cca 622 KB)

Zde najdete informace o frameworku, na němž funguje poštovní server i5/OS.

IBM Redbooks

- AS/400 Electronic-Mail Capabilities (cca 3593 kB)
  V této populární publikaci IBM Redbooks najdete podrobné informace o e-mailu a SMTP.
- AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet (cca 2160 KB)
  Tento Redbook obsahuje informace o zabezpečení ochrany, včetně kroků potřebných pro vyčištění systému i5/OS po napadení způsobujícím jeho zahlcení.

Webové stránky

- Support for IBM System i
  Stáhněte si aktuální PDF pro váš operační systém i5/OS pomocí pracovní stanice, kterou použijte jako bránu k internetové stránce s PTF, nebo si prohlédněte řešení pro i5/OS pod tématem Technické informace a databáze.
- RFC Index
  Protokoly elektronické pošty jsou definovány v prostředí RFC (Request for Comments). RFC jsou nástroje, které se používají pro definování vyvíjených internetových standardů. Další informace o SMTP naleznete v RFC 1939 (POP3), RFC 2449 (POP3 Extension Mechanism) a RFC 2595 (Using TLS with IMAP, POP3 and ACAP).
- Lotus Domino for i5/OS
  Tato webová stránka představuje produkt Lotus Domino for i5/OS a řešení, která tento licencovaný program poskytuje.
- Lotus Domino Reference Library
  Další informace o produktu Domino naleznete v dokumentech White paper, příručkách, prezentacích.
- Lotus Documentation
  Stránky s dokumentací produktu Lotus poskytují odkazy ke zdrojům, jako je například produktová dokumentace, dokumenty White paper, publikace Redbooks publications, a další.

Další informace

System i a zabezpečení Internetu

Prohlédněte si tuto kolekci témat v aplikaci Informační centrum, chcete-li zabezpečit síť systému System i.

Související odkazy

“Soubor ve formátu PDF pro publikaci E-mail” na stránce 2
Soubor s těmito informacemi ve formátu PDF si můžete zobrazit a vytisknout.

Dodatek. Poznámky

Tyto informace jsou určeny pro produkty a služby nabízené ve Spojených státech.

Společnost IBM nemusí v ostatních zemích nabízet produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou v současné době dostupné ve Vaší oblasti, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená ani z něj nelze vyvozovat, že smí být použit pouze tento produkt, program či služba IBM. Použít lze jakýkoliv funkčně ekvivalentní produkt, program či službu, které neporušují práva IBM na duševní vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

Společnost IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zasílat na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení společnosti IBM ve své zemi, nebo písemně zastoupení IBM na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Následující odstavec neplatí pro Velkou Británii a další země, ve kterých tato opatření nejsou v souladu s místními právními předpisy: IBM POSKYTUJE TUTO PUBLIKACI " JAK JE" (AS-IS), BEZ JAKÝCHKOLI ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk vyjádřených výslovně nebo vyplývajících z okolností v určitých transakcích, a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. Společnost IBM má právo kdykoliv, bez upozornění zdokonalovat nebo měnit produkt(y) a program(y) popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro potřeby uživatelů a v žádném případě neslouží jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo šířit veškeré Vámi poskytnuté informace libovolným způsobem, který pokládá za vhodný, aniž by jí z toho plynuly nějaké závazky vůči Vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v tomto dokumentu a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě pro programy, v Mezinárodní licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Jakékoli zde obsažené údaje o výkonu byly získány v kontrolovaném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou podstatným způsobem lišit. Některá měření mohla být provedena v systémech na úrovni vývoje a nelze zaručit, že tato měření budou stejná v obecně dostupných systémech. Kromě toho mohly být některé hodnoty odhadnuty pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé této příručky by měli ověřit použitelnost dat pro konkrétní prostředí.

Informace týkající se produktů jiných firem než IBM byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM tyto produkty netestovala a nemůže tedy potvrdit přesnost údajů o výkonu, kompatibilitě a další prohlášení vztahující se k těmto produktům jiných dodavatelů. Dotazy, které se týkají vlastností produktů jiných firem než IBM, musí být adresovány jejich dodavatelům.

Veškerá prohlášení týkající se budoucího směřování a záměrů společnosti IBM může IBM bez předchozího oznámení změnit nebo zcela odvolat a tato prohlášení představují pouze cíle a plány.

Tento dokument obsahuje příklady dat a sestav používaných v běžném firemním provozu. Z důvodu jejich co nejúplnější ilustrace obsahují příklady jména osob a názvy firem, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jakákoliv podobnost se jmény, názvy a adresami skutečné firmy je čistě náhodná.

LICENČNÍ INFORMACE - COPYRIGHT:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které demonstrují techniku programování v různých operačních systémech. Tyto vzorové programy můžete kopírovat, modifikovat a distribuovat v jakékoliv formě za účelem vývoje, používání, propagace nebo distribuce aplikačních programů, které odpovídají aplikačnímu programovému rozhraní pro daný operační systém, pro nějž byly vzorové programy napsány, a to bez jakýchkoli poplatků IBM. Tyto příklady nebyly náležitě testovány pro všechny podmínky. IBM proto nezaručuje ani nenaznačuje spolehlivost, provozuschopnost a funkčnost těchto programů.

Každá kopie nebo kterákoli část uvedených vzorových programů nebo jakékoliv odvozené dílo musí obsahovat informaci o copyrightu v tomto formátu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu byly odvozeny ze vzorových programů společnosti IBM Corp. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Informace o programových rozhraních

Publikace E-mail dokumentuje plánovaná programovací rozhraní, která zákazníkovi umožňují psát programy za účelem získání služeb systému IBM i5/OS.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM ve Spojených státech a případně v dalších jiných zemích.

AIX
AS/400
Domino
eServer
i5/OS
IBM
IBM (logo)
Infoprint
iSeries
Lotus
Lotus Notes
Redbooks
System i
Výstup e-business
Tivoli

Adobe, logo Adobe, PostScript a logo PostScript jsou buď registrované ochranné známky nebo ochranné známky společnosti Adobe Systems Incorporated ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou registrované ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Java a všechny ochranné známky obsahující slovo Java jsou ochranné známky společnosti Sun Microsystems, Inc. ve Spojených státech a případně v dalších jiných zemích

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI,

NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.