Systémy IBM - iSeries

Správa systémů
Začínáme s Centrální správou

Verze 5, vydání 4

Systémy IBM - iSeries

Správa systémů
Začínáme s Centrální správou

Verze 5, vydání 4

Poznámka

Před použitím této příručky a produktů, jichž se týká, si přečtěte informace v části “Poznámky”, na stránce 17.

Sedmé vydání (únor 2006)

Toto vydání se vztahuje k verzi 5, vydání 4, modifikaci 0 operačního systému IBM i5/OS (číslo produktu 5722-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

Centrální správa

Zajímá vás, jak dosáhnout toho, aby správa vašeho systému byla jednodušší, snazší, méně časově náročná a méně opakovaná? Hledáte způsob, jak snížit celkové náklady na provozování serveru? Produkt iSeries Navigator poskytuje technologii, kterou potřebujete pro úlohy správy systému prováděné na jednom serveru nebo více serverech simultánně.

Klepnutím na položku Centrální správa v prostředí produktu iSeries Navigator zobrazíte sadu snadno použitelných funkcí správy systému, které máte k dispozici jako součást základního operačního systému. Centrální správu v prostředí produktu iSeries Navigator můžete používat pro správu jednoho nebo více systémů pomocí jediného centrálního systému. Vyberte server, který budete používat jako centrální systém, a pak přidejte koncové systémy do své sítě Centrální správy. Chcete-li si usnadnit správu systému, můžete vytvářet skupiny podobných nebo příbuzných koncových systémů. Komunikaci za vás bude vyřizovat váš centrální systém. Můžete také využít takové volby, jako je například plánování a neobsluhované operace. Nepochybně zjistíte, že Centrální správa je flexibilní a snadno obsluhovatelný nástroj, který vyhoví vašim potřebám.

S produktem iSeries Navigator for Wireless získají administrátoři větší flexibilitu, pokud jde o jejich přístup k Centrální správě a o to, jak s ní budou pracovat. Pokyny a doporučení, jaká zařízení použít, jak nainstalovat a nakonfigurovat požadované prvky, naleznete v tématu s přehledem o produktu iSeries Navigator for Wireless.

Související informace

Přehled produktu iSeries Navigator for Wireless

Začínáme s Centrální správou

Chcete-li Centrální správu využít co nejlépe, nastavte svůj centrální systém a koncové systémy v souladu s požadavky a potřebami vašeho obchodního prostředí. Jakmile dokončíte tyto předběžné kroky, můžete začít pracovat s Centrální správou.

Vytisknutelný dokument PDF části: **Začínáme s Centrální správou** (cca 234 kB).

Související informace

Instalace produktu iSeries Navigator

Dříve než začnete

Tato sada témat obsahuje informace, které vám pomohou snadno dokončit instalaci a úspěšně připojit Centrální správu. Důrazně doporučujeme, abyste si před instalací přečetli všechny informace v této sadě.

Související informace

Servisní webové stránky produktu iSeries Navigator

Nastavení časové zóny před přechodem na vyšší verzi

Zpráva o zkušenosti: Configuring Management Central Connections for Firewall Environments

Nastavení protokolu TCP/IP

Odstraňování problémů s protokolem TCP/IP

Konfigurace kontrolního seznamu předpokladů TCP (CFGTCP)

Chcete-li zajistit hladkou instalaci a nastavení Centrální správy, musíte náležitě připravit prostředí. Před instalací Centrální správy se pomocí kontrolního seznamu v tomto tématu ujistěte, že je vše připraveno.

Kontrolní seznam předpokladů

1. Server iSeries je aktuální pouze s nejnovějšími opravami, servisními balíky a skupinou oprav Java PTF.
2. Přečtěte si stránku Frequently Asked Questions na servisních webových stránkách produktu Navigator.

3. V případě operačního systému OS/400 V5R2 a staršího použijte k nastavení časové zóny serveru Java systémovou hodnotu QTIMZON. (Protože v libovolném systému verze V5R3 nebo novější se systémová hodnota QTIMZON používá k určení časové zóny serveru Java.)
4. Zaveďte všechny klienty produktu iSeries Navigator a nejnovější servisní balíky. (Vydání klienta může být vyšší než vydání centrálního systému.)
5. Určete IP adresy všech klientů, které budete používat. Pokud má klient vícenásobnou IP adresu, pravděpodobně bude třeba nastavit IP adresu, kterou má centrální systém použít k připojení k počítači. V takovém případě se IP adresa, která má být použita, určí nastavením hodnoty QYPS_HOSTNAME v souboru MgmtCtrl.properties. Pomocí následujících kroků určíte, která IP adresa bude fungovat. Použijte k tomu příkaz IPCONFIG na příkazovém řádku systému DOS. Adresy si poznamenejte pro případné budoucí použití.
   a. Potvrďte platné připojení z počítače k centrálnímu systému. V počítači zadejte příkaz ping (ping xx.xx.xx.xx, kde x je IP adresa centrálního systému).
   b. Na příkazovém řádku počítače spusťte příkaz IPCONFIG a zaznamenejte si všechny IP adresy.
   c. V centrálním systému spusťte příkaz ping na každou IP adresu.
   d. Pro první IP adresu, která funguje, vytvořte soubor C:\MgmtCtrl.properties a přidejte do něj tento řádek: QYPS_HOSTNAME==<IP adresa, na kterou jste spustili příkaz ping>.
6. Přecházíte-li na vyšší verzi produktu iSeries Navigator, zavřete všechna jeho otevřená okna ukončete ho. Spusťte produkt iSeries Navigator a zkuste se připojit k centrálnímu systému.

Otázky týkající se připojení Centrální správy

Pochopení toho, jak Centrální správa vytváří připojení, je důležitou podmínkou úspěšné instalace a nastavení. Ať už je konfigurace vašeho systému jednoduchá nebo složitá, na úspěšné připojení má vliv mnoho aspektů.

Jak Centrální správa vytváří připojení

Po svém spuštění server Java Centrální správy (QYPSJSVR) získá své IP adresy z protokolu TCP/IP pomocí dlouhého jména (systém + název domény). Klienti, kteří se objeví pod položkou Připojení, a koncové body Centrální správy se obvykle definují pomocí jména systému a krátkého jména.

Předvolená frekvence vyhledávání produktu iSeries Navigator je *Vždy*. Toto nastavení způsobí, že systém uvedený po položkou Připojení použije k určení IP adresy DNS nebo tabulku hostitelů TCP/IP (příkaz CFGTCP (Konfigurování TCP/IP), volba 10) tak, aby se mohl připojit k centrálnímu systému. Priorita vyhledání názvu hostitele (příkaz CFGTCP (Konfigurování TCP/IP), volba 12) řídí způsob prohledání DNS. Je-li nastavena na hodnotu *LOCAL, bude se nejprve prohledávat tabulka hostitelů TCP/IP. Pokud zde adresa není nalezena, použije se DNS. Je-li priorita nastavena na hodnotu *REMOTE, bude se nejprve prohledávat DNS a pak tabulka hostitelů TCP/IP.

Časový limit připojení

Nejsou-li na určitém koncovém bodu spuštěny servery Centrální správy, dojde k okamžitému selhání připojení. Pokud je však systém mimo provoz nebo se použije chybná IP adresa, nelze vytvořit připojení, a před zobrazením selhání připojení uplyne několikaminutový časový limit.

Testy připojení

Centrální správa používá k připojení k centrálnímu systému IP adresu systému pod položkou Připojení. Při testu připojení Centrální správa spustí příkaz ping na počítač se jménem, které se používá pro centrální systém (obvykle se jedná o krátké jméno), a pak pomocí dlouhého jména vrátí IP adresu stejnou jako příkaz ping na centrální systém. Není-li tento postup úspěšný, nemůže se klient připojit k serveru Java. Tento problém lze vyřešit přepsáním IP adresy centrálního systému.

Chcete-li přepsat IP adresu centrálního systému, použijte následující znakově orientovaný příkaz:

```
CALL PGM(QSYS/QYPSCONFIG) PARM(xxxx 'y.y.y.y')
```

Kde xxxx je nastavení QYPSHOSTNAME a y.y.y.y je hodnota IP adresy, která se má použít.

Důležité: Soubor upravte pomocí znakově orientovaného rozhraní. Nepoužívejte mapovanou jednotku nebo jinou metodu.

Frekvence vyhledávání

Frekvenci vyhledávání Centrální správy nastavuje systémová proměnná prostředí QYPS_DNS (0 = Nikdy, 1 = Vždy). Systémovou proměnnou QYPS_DNS můžete nastavit jedním z těchto způsobů:

- Okno vlastností Centrální správy.
- Karta Připojení v klientovi.
- Pomocí znakově orientovaného rozhraní přidejte proměnnou prostředí:

```
CALL PGM(QSYS/QYPSCONFIG) PARM(xxxx 'y')
```

Kde QYPS_DNS je nastavení a y je hodnota 0 nebo 1.

Doporučuje se frekvenci vyhledávání nastavit na hodnotu Vždy. Je-li frekvence vyhledávání nastavena na hodnotu Vždy, je IP adresa ve vlastnostech koncového bodu ignorována a zadá se požadavek na získání adresy prostřednictvím DNS nebo tabulky hostitelů v centrálním systému. Výsledkem je to, že Centrální správa vybere novou IP adresu, i když dojde ke změně IP adres či ke změně DNS nebo tabulky hostitelů.

Je-li frekvence nastavena na hodnotu Nikdy, použije se IP adresa uložená ve vlastnostech koncového objektu. V důsledku toho je možné, že se klient úspěšně připojí k centrálnímu systému, který používá IP adresu uloženou v položce Připojení, ale pak když spustí úlohu v centrálním systému, dojde k selhání připojení. Taková událost naznačuje, že frekvence vyhledávání Centrální správy je nastavena na hodnotu Nikdy a že IP adresa v koncovém bodu pro centrální systém je nesprávná. Tuto situaci vyřešíte úpravou IP adresy pro koncový bod v okně vlastností koncového bodu.

Poznámka: Nastavení frekvence vyhledávání Centrální správy a nastavení frekvence vyhledávání pro systém pod položkou Připojení jsou dvě různá nastavení.

Připojení k serveru Java

Když se klient připojuje k serveru Java, použije server Java proceduru autentizace, která se připojí zpět k PC. Proto centrální server musí být schopen spustit příkaz ping na PC.

K obvyklým problémům s připojením dochází tehdy, když je adresa počítače rezervovaná pro soukromé sítě (například v případě, kdy uživatel používá k přístupu do sítě za směrovačem síť VPN). Předpokládejme například, že adresa počítače je 10.100.46.143 a IP adresa centrálního systému je 164.143.28.82. Dojde k selhání připojení, protože adresy začínající číslem 10 nejsou směrovačem předávány. V takové situaci musíte zjistit externí IP adresu počítače, vytvořit v klientovi soubor C:\MgmtCtrl.properties a přidat do něj řádek QYPS_HOSTNAME=xxx.xxx.xxx.xxx (kde xxx.xxx.xxx.xxx je externí IP adresa počítače). Poté server Java použije k připojení k počítači IP adresu zadanou v souboru vlastností.

Otázky týkající se hromadných přenosů dat v Centrální správě

Hromadný přenos je funkce, která v Centrální správě slouží k přenosu dat ze zdrojového systému do cílového (jedná se například o odeslání sady, oprav PTF atd.). K úspěšnému přenosu je třeba, aby byl cílový systém schopen se připojit zpět ke zdrojovému systému. IP adresa použitá v cílovém systému je určena frekvencí vyhledávání v cílovém systému. Je-li frekvence vyhledávání nastavena na hodnotu Nikdy, použije se IP adresa poskytnutá centrálním systémem pro zdrojový systém. Je-li frekvence vyhledávání v cílovém systému nastavena na hodnotu Vždy, pak k určení IP adresy zdrojového systému bude použit server DNS nebo tabulka hostitelů.

Spouštění úloh Centrální správy z položky Připojení

Některé z funkcí produktu iSeries Navigator používají k získávání informací Centrální správu. Opravy PTF v Soupisu můžete například zobrazit pomocí voleb **Připojení → Konfigurace a služba**. Nemůže-li se Centrální správa připojit k

centrálnímu systému, pak u funkce, kterou se pokoušíte použít, dojde k několikaminutové prodlevě. Výsledkem je zpráva o selhání připojení. Spolehlivým postupem je rozbalení Centrální správy dříve, než spustíte jakoukoli její funkci umístěnou pod položkou Připojení. Tímto postupem se ujistíte, že je možné se připojit k centrálnímu systému.

Chcete-li spustit úlohu Centrální správy v systému pod položkou Připojení, musí být tento systém také definovaný jako koncový bod pod Centrální správou. Chcete-li systém definovat jako koncový bod, rozbalte **Centrální správa → klepněte pravým tlačítkem na Koncové systémy → Nový koncový systém**.

Instalace a přístup k Centrální správě

Po dokončení všech předem požadovaných úloh můžete nainstalovat Centrální správu. Tato řada témat se zabývá instalačními kroky a způsobem fungování funkce připojení. Pokud se po instalaci Centrální správy nezdaří připojení, přečtěte si řadu článků o odstraňování problémů s jejím připojením.

Proč je vyžadováno nejnovější vydání Centrální správy?

Každé nové vydání Centrální správy obsahuje aktualizované funkce, prvky a opravy, které Centrální správě dávají schopnost spravovat systém s počítači, ve kterých jsou spuštěny různé verze operačního systému i5/OS. Chcete-li tyto nové funkce používat, musíte mít nejnovější vydání Centrální správy a její závislosti.

Kontrola aktuálnosti kódu Centrální správy

Chcete-li úspěšně používat Centrální správu, musíte mít aktuální kód jejího serveru a klienta a její závislosti.

Kontrola, zda mají servery Centrální správy aktuální kód

Souhrn doporučených oprav podle vydání obsahují dokumenty: IBM Software Technical Document, Recommended PTFs for Management Central a dokument číslo 360059564.

Chcete-li na tuto stránku přejít z webové stránky IBM (www.ibm.com), postupujte takto:

1. Na řádkovém menu klepněte na **Products**.
2. Na stránce Products, pod položkou Servers klepněte na **Midrange (iSeries)**.
3. Na stránce Midrange systems: iSeries na navigačním panelu umístěném na levé straně klepněte na **Support**.
4. Na stránce Support for iSeries family na navigačním panelu umístěném na levé straně klepněte na iSeries support search.
5. Do pole **Search for** zadejte číslo dokumentu a klepněte na **Search**.

Kontrola, zda má klient Centrální správy aktuální kód

Aktuální informace o servisních balících (opravách) pro produkt iSeries Access for Windows poskytuje stránka iSeries Access. Chcete-li na tuto stránku přejít z webové stránky IBM (www.ibm.com), postupujte takto:

1. Na řádkovém menu klepněte na **Products**.
2. Na stránce Products, pod položkou Servers klepněte na **Midrange (iSeries)**.
3. Na stránce Midrange systems: iSeries na navigačním panelu umístěném na levé straně klepněte na **Software**.
4. Na stránce iSeries Software klepněte na kartu Overview (není-li již vybrána) a pak klepněte na **iSeries Software A-Z**.
5. Pod písmenem A klepněte na **iSeries Access**.
6. Na stránce iSeries Access na navigačním panelu umístěném na levé straně klepněte na **Service Packs (Fixes)**.

Související úlohy

"Změna nastavení centrálního systému" na stránce 12
Jako centrální systém si můžete kdykoli zvolit jiný systém. Centrální systém musí být takový systém, k němuž jste přímo připojeni. Chcete-li používat nejnovější funkce produktu iSeries Navigator, musí být ve vašem centrálním systému spuštěn operační systém i5/OS verze 5, vydání 4 (V5R4).

Postup instalace a získání přístupu k Centrální správě

Některé funkce pro správu systémů, které budete chtít používat, jsou volitelně instalovatelnými komponentami produktu iSeries Navigator - grafického uživatelského rozhraní pro servery iSeries.

Vyberete-li v průvodci instalací volbu Typická, nainstalují se následující funkce Centrální správy.

- Úlohy (pouze soupis).
- Koncové systémy.
- Skupiny systémů.

Pokud jste nenainstalovali všechny potřebné komponenty už při instalaci programu iSeries Navigator, postupujte následovně:

1. V řádkovém menu produktu iSeries Navigator vyberte **Soubor → Volby instalace → Výběrová instalace**.
2. Průvodcem Výběrová instalace nainstalujte další komponenty, které potřebujete pro funkce pro správu systémů. Chcete-li využívat všechny funkce pro správu systémů, vyberte položky Konfigurace a služba, Uživatelé a skupiny, Příkazy, Sady programů a produkty a Monitory.

   Když použijete průvodce výběrovou instalací, nainstalují se komponenty, které vyberete. Všechny komponenty, u nichž zrušíte označení, se při výběrové instalaci odinstalují. Při používání průvodce výběrovou instalací musíte být opatrní, abyste omylem nic neodinstalovali.

Jakmile jste nainstalovali produkt iSeries Navigator, spusťte jej dvojitým klepnutím na jeho ikonu na pracovní ploše. Nyní jste připraveni k nastaveni centrálního systému.

Související informace

Produkt iSeries Navigator

Instalace produktu iSeries Access for Windows

Funkce ověření připojení

Funkce Ověřit připojení v Centrální správě a Ověřit připojení pod položkou Připojení jsou dvě různé funkce. Toto téma rozebírá jejich účel a odlišnosti.

Funkce Ověřit připojení pod položkou Připojení

Připojení → klepněte pravým tlačítkem na server → Diagnostika → Ověřit připojení

Tato funkce Ověřit připojení spustí příkaz ping na jednotlivé hostitelské servery, aby zjistila, zda jsou zapnuté a správně spuštěné a zda jsou dostupné z PC. Jelikož je omezena na funkce jednoho systému produktu Navigator, je to jedna z prvních věcí, kterou byste měli při odstraňování problémů se selhaným připojením Centrální správy vyloučit. (Mnoho funkcí Centrální správy je založeno na funkcích jednoho systému.) Po té, co jste pod položkou Připojení potvrdili, že připojení ke koncovým systémům je úspěšné, můžete pokračovat ověřením připojení z Centrální správy.

Funkce Ověřit připojení v Centrální správě

Klepněte pravým tlačítkem na Centrální správu → Ověřit připojení

Funkce Ověřit připojení v Centrální správě představuje diagnostický nástroj k prověření nejběžnějších faktorů přispívajících k selhání připojení. Po dokončení zobrazuje stav těchto testů. Pokud ohlásí selhání, získáte další informace o selhání a také o obnově klepnutím na volbu **Podrobnosti**. Níže je uveden seznam toho, co Centrální správa ověřuje.

- Nastavení serveru Java v centrálním systému je správné (to zahrnuje ověření přítomnosti určitých souborů .jar a toho, zda nedošlo ke změně určitých integrovaných oprávnění k souborům a složkám v souborovém systému).
- Požadované soubory dodané s operačním systémem nebyly z centrálního systému vymazány, nejsou poškozeny a jsou zapisovány do žurnálu.
- Konfigurace protokolu TCP/IP v centrálním systému je platná (to zahrnuje ověření, zda jsou jména hostitelů centrálního systému i PC v tabulce hostitelů případně v DNS.

- Lze provést jednoduché připojení produktu Navigator k centrálnímu systému.
- VRM, jméno hostitele, IP adresa centrálního systému a VRM produktu iSeries Navigator.
- Porty používané Centrální správou nepoužívá jiná aplikace centrálního systému.
- Uživatelské profily v centrálním systému potřebné ke spuštění Centrální správy nebyly vymazány nebo zakázány a mají platná hesla s nevypršenou platností.
- Vrstva SSL je správně nakonfigurována (pokud je v centrálním systému používána) a jak PC, tak centrální systém vrstvu SSL používají.
- Centrální systém není v prostředí Vysoké dostupnosti v Centrální správě označený jako sekundární systém (sekundární systémy nelze použít jako centrální systémy).
- Servery Centrální správy v centrálním systému jsou zapnuté a spuštěné.
- Ohlásí, jaké typy autentizace jsou v centrálním systému podporovány.

Poznámka:

Ke spuštění funkce Ověřit připojení Centrální správy v klientovi (PC) produkt iSeries Navigator používá kód produktu Java Toolbox. Pokud kód produktu Toolbox nefunguje správně, funkce Ověřit připojení se nespustí. Pokud v serveru správně nefunguje produkt Java Virtual Machine (JVM) nebo kód produktu Toolbox, bude funkce Ověřit připojení pracovat až do několika posledních kontrol. K provedení několika posledních kontrol je nutné spustit produkt JVM.

Související informace

Produkt IBM Toolbox for Java

Nastavení centrálního systému

Chcete-li spravovat více serverů z jednoho systému, potřebujete mít centrální systém. Po instalaci Centrální správy a po úspěšném připojení můžete nastavit centrální systém.

Serverům ve vaší síti se říká *koncové systémy*. Jeden z těchto koncových systémů si vyberte jako svůj centrální systém. Jakmile přidáte koncové systémy do své sítě a vyberete si centrální systém, můžete své úlohy správy systému provádět už pouze jednou. Váš centrální systém bude iniciovat vaše úlohy a ukládat veškerá data nezbytná ke správě systémů. Centrální systém si zvolíte při prvním spuštění produktu iSeries Navigator. Centrální systém můžete později kdykoli snadno změnit.

Důležité: Vydání centrálního systému musí představovat nejvyšší vydání v síti.

První nastavení centrálního systému

Chcete-li začít používat produkt iSeries Navigator, klepněte dvakrát na ikonu na pracovní ploše a vyberte server iSeries, k němuž se chcete připojit, a definujte připojení k serveru iSeries. První server, který zadáte, se přiřadí jako váš centrální systém. Centrální správa se objevuje automaticky nahoře v seznamu, v levé části okna iSeries Navigator. Server Centrální správy se automaticky spouští na centrálním systému.

Chcete-li získat přístup k funkcím distribuované správy systému v prostředí produktu iSeries Navigator, rozbalte položku **Centrální správa**.

| V případě systémů s operačním systémem i5/OS V5R3 a novějším jsou databáze Centrální správy umístěné v
| knihovnách QMGTC a QMGTC2. V případě systémů s operačním systémem starším než i5/OS V5R3 jsou databáze
| Centrální správy umístěné v knihovně QUSRSYS.

| K dokončení inicializace server Centrální správy vyžaduje, aby byl uživatelský profil QSECOFR povolený a aktivní.
| Jestliže použijete jiné jméno profilu se stejnými právy jako profil QSECOF, musíte v centrálním systému spustit tento
| příkaz:

```
| CALL PGM(QSYS/QYPSCONFIG) PARM(QYPSJ_SYSTEM_ID 'XXXXX')
```

| (xxxxx je ID uživatele jiné než předvolené QSECOFR.)

V některých případech může mít centrální systém více IP adres, pomocí kterých k němu lze získat přístup. (CFGTCP, volba 10). K zobrazení IP adresy, která bude vrácena Centrální správě, můžete v centrálním systému použít příkaz ping. Pokud se nejedná o IP adresu, kterou klienti používají k připojení k systému, můžete předvolenou adresu přepsat adresou zobrazenou příkazem ping. K přepsání předvolené IP adresy lze použít následující příkaz:

```
CALL PGM(QSYS/QYPSCONFIG) PARM(QYPS_HOSTNAME 'w.x.y.z')
```

(w.x.y.z je IP adresa, kterou by Centrální správa měla použít k připojení.)

Je-li v centrálním systému spuštěn systém OS/400 V5R2 nebo novější (nebo V5R1 s opravou PTF SI06917), klepněte pravým tlačítkem na volbu **Centrální správa** a vyberte volbu **Ověření připojení**. Tím ověříte správnost konfigurace připojení centrálního systému. Chcete-li zobrazit podrobné informace zprávy o selhání, vyberte zprávu a klepněte na **Podrobnosti** (nebo dvakrát klepněte na zprávu).

Poznámka: Funkce Ověření připojení pouze potvrdí, že Centrální správa v centrálním systému správně funguje. Úspěšnému připojení Centrální správy k centrálnímu systému může také zabránit konfigurace protokolu TCP/IP a ochranné bariéry.

Další informace o těchto a jiných úlohách a tématech Centrální správy naleznete v podrobné nápovědě k úlohám, která je dostupná v prostředí produktu iSeries Navigator. Na řádkovém menu klepněte na **Nápověda** a vyberte **Přehled produktu iSeries Navigator → Centrální správa**.

Související informace

Zpráva o zkušenosti: Configuring Management Central Connections for Firewall Environments

Odstraňování problémů s protokolem TCP/IP

Nastavení protokolu TCP/IP

Scénáře týkající se SSL

Nastavení a volby Centrální správy

Při migraci z vydání staršího než V5R3 si musíte uvědomit, že proměnné prostředí byly přemístěny. Toto téma popisuje, kde najít proměnné prostředí klienta a serveru v případě systémů s vydáním V5R3 či starším.

/QIBM/UserData/OS400/Mgtc/Config/McCSConfig.properties

QYPS_EARLIEST_RELEASE
QYPS_MAXPTF_SIZE
QYPS_FTP_DISCOVERY
QYPS_DISCOVERY_TIMEOUT
QYPS_DISC_LCLSUBNET
QYPS_SNMP_DISCOVERY
QYPS_IP_DISCOVERY
QYPS_DISCOVERY_STARTUP
QYPS_MAX_SOCKETS
QYPS_MAX_CONTIMOUT
QYPS_RETRY_TIMEOUT
QYPS_RETRY_INTERVAL
QYPS_AUTORETRY
QYPS_SOCKETTIMEOUT
QYPS_COLLECTPTF_IFCHANGED
QYPS_DNS
QYIV_QUERY_MAX_SIZE
QYPSJ_SAVF_RECORDS
QYPSJ_TOOLBOX_TRACE
QYPS_LOCATION
QYPS_LOCATION2
QYPSJ_CONNECT_INTERVAL

/Qibm/UserData/OS400/Mgtc/Config/McCSSecure.properties

(nastavení SSL)

QYPS_AUTH_LEVEL
QYPS_SSL

/Qibm/UserData/OS400/Mgtc/Config/McEPConfig.properties

QYPS_TRACE
QYPSJ_TRACE
QYPSJ_SYSTEM_ID
QYPS_MAX_TRANSFERS
QYPS_HOSTNAME
QYPS_MINIMUM_PORT
QYPS_MAXIMUM_PORT

/Qibm/UserData/OS400/Mgtc/Config/McEPSecure.properties

QYPS_USER_PASSWORD
QYPS_BASIC_AUTH
QYPS_TRUST_LEVEL
QYPS_KERBEROS_PRINCIPAL
QYPS_KERBEROS_CONFIG
QYPSJ_SYSTEM_ID
QYPS_ID_MAPPING_ONLY
QYPS_USE_ID_MAPPING

Nastavení

Produkt iSeries Navigator vám v prostředí sítě TCP/IP umožňuje spravovat více serverů z jediného systému. Některé aspekty vašeho prostředí TCP/IP mohou vyžadovat změny konfigurace serveru Centrální správy. Pokud například používáte ochrannou bariéru nebo chcete používat šifrování SSL pro komunikace serveru Centrální správy, možná budete muset změnit některá nastavení serveru Centrální správy.

Tabulka 1. Nastavení Centrální správy nastavovaná prostřednictvím produktu iSeries Navigator

Jméno	Popis	Hodnoty	Jméno pole v produktu iSeries Navigator (klepněte pravým tlačítkem na Centrální správa → Vlastnosti → karta Připojení)
QYPS_AUTORETRY	Určuje, zda provést automatické restartování monitorů v selhaných systémech.	0 = Ne, 1 = Ano	Automaticky znovu spustit monitory v systémech, které selhaly
QYPS_COLLECTPTF_IFCHANGED	Aktualizovat soupis oprav pouze v případě, že nastaly změny.	0 = Ne, 1 = Ano; 0 je předvolená hodnota	Při shromažďování soupisu provést aktualizaci pouze v případě, že nastaly změny
QYPS_DNS	Frekvence vyhledávání IP adresy	0 = Nikdy, 1 = Vždy	Frekvence vyhledávání IP adresy
QYPS_MAX_CONTIMOUT	Maximální doba čekání (v sekundách) na vytvoření připojení k systému.	1 až 3600 (Předvolená hodnota je 180 sekund.)	Během připojení ke koncovým systémům
QYPS_MAX_SOCKETS	Maximální počet soketů, které lze v systému vytvořit.	200 (Toto je předvolená hodnota.)	Maximum připojení
QYPS_MAXPTF_SIZE	Maximální velikost přenosu dat.	-1 = žádná maximální velikost	Maximální velikost přenosu dat (MB)
QYPS_RETRY_INTERVAL	Udává, jak často (v minutách) má dojít k pokusu o restart monitoru.	5 (Toto je předvolená hodnota.)	Jak často se pokoušet o restart
QYPS_RETRY_TIMEOUT	Udává, jak dlouho (v minutách) má docházet k pokusům o restart monitoru.	180 (Toto je předvolená hodnota.)	Jak dlouho se pokoušet o restart
QYPS_SOCKETTIMEOUT	Maximální doba čekání (v sekundách) na to, až se soket vrátí z požadavku.	30 sekund (Toto je předvolená hodnota.)	Při připojování ke koncovým systémům

Tabulka 2. Nastavení Centrální správy nastavená prostřednictvím znakově orientovaného rozhraní

Jméno	Popis	Hodnoty	Použijte znakově orientované rozhraní.
QYIV_QUERY_MAX_SIZE	Maximální počet záznamů v dotazu na soupis	200	
QYPS_HOSTNAME	Jméno hostitele nebo IP adresa, ke kterým se mají koncové body a počítače připojovat v případě, že potřebují nové připojení zpět k systému. **Poznámka:** Použijete-li jméno hostitele, spoléháte na to, že koncový bod nebo počítač jméno hostitele rozpozná pomocí své tabulky hostitelů nebo DNS.		
QYPS_LOCATION	Jméno knihovny, kde se nacházejí databáze Centrální správy.	QMGTC	
QYPS_LOCATION2	Jméno druhé knihovny, kde se nacházejí databáze Centrální správy.	QMGTC2	
QYPS_ID_MAPPING_ONLY	Určuje, zda se má pro autentizaci použít pouze technologie EIM (Enterprise Identity Mapping).	0 = Ne, 1 = Ano	
QYPS_MAXIMUM_PORT	Používáno úlohou BDT (Bulk Data Transfer) QYPSBDTSVR. Maximum rozsahu čísel portu, který se má použít.		
QYPS_MINIMUM_PORT	Používáno úlohou BDT (Bulk Data Transfer) QYPSBDTSVR. Minimum rozsahu čísel portu, který se má použít.	Jméno serveru hostitele.	
QYPS_TRACE	Trasování serveru C++.	-1 vypnutí, 0 zapnutí	
QYPS_USE_ID_MAPPING	Trasování serveru Java.	-1 vypnutí, 2 zapnutí	
QYPSJ_CONNECT_INTERVAL	Jak často (ve vteřinách) provést kontrolu připojení.	60	
QYPSJ_PORT	Port, na kterém server Java naslouchá příchozím požadavkům klientů.	5544 (Toto je předvolená hodnota.)	
QYPSJ_SAVF_RECORDS	Maximální počet záznamů v souboru typu save file serveru Java.	100	
QYPSJ_SYSTEM_ID	Uživatelský profil s oprávněním ke všem objektům.	Uživatelský profil, který server Java spouští pro určité úlohy. Teto profil musí mít třídu oprávnění *SECOFR. Předvolený uživatelský profil je QSECOFR, případně můžete zadat jméno uživatelského profilu.	
QYPSJ_TOOLBOX_TRACE	Určuje, zda se má zapnout trasování produktu Toolbox.	0 = vypnuto, 1 = zapnuto	
QYPSSRV_PORT	Port, na kterém server C++ naslouchá příchozím požadavkům klientů.	5555. (Toto je předvolená hodnota.)	
QYPSJ_TRACE	Port, na kterém server C__ naslouchá příchozím požadavkům klientů.	Předvolená hodnota je 5555.	

Tabulka 3. Nastavení Centrální správy nastavovaná prostřednictvím produktu iSeries Navigator

Jméno	Popis	Hodnoty	Jméno pole v produktu iSeries Navigator (Centrální správa → klepněte pravým tlačítkem na Koncové systémy → Vlastnosti)
QYPS_DISC_LCLSUBNET	Objevení lokální podsítě.	0 = Ne, 1 = Ano	
QYPS_DISCOVERY_STARTUP	Prohledávat při každém spuštění Centrální správy.	0 = Ne, 1 = Ano	
QYPS_DISCOVERY_TIMEOUT	Časový limit objevení (ve vteřinách).	15 (Toto je předvolená hodnota.)	Časový limit (vteřiny)
QYPS_EARLIEST_RELEASE	Nejstarší vydání operačního systému k vyhledání.	Předvolená hodnota je V5R4M0.	Nejstarší vydání operačního systému k vyhledání
QYPS_FTP_DISCOVERY	Spuštění vyhledávání pomocí protokolu FTP (File Transfer Protocol).	0 = Ne, 1 = Ano	Zaškrtávací okénko protokolu FTP: Jak ověřit systémy
QYPS_IP_DISCOVERY	Spuštění vyhledávání pomocí protokolu IP (Internet Protocol).	0 = Ne, 1 = Ano	

Tabulka 3. Nastavení Centrální správy nastavovaná prostřednictvím produktu iSeries Navigator (pokračování)

Jméno	Popis	Hodnoty	Jméno pole v produktu iSeries Navigator (Centrální správa → klepněte pravým tlačítkem na Koncové systémy → Vlastnosti)
QYPS_SNMP_DISCOVERY	Spuštění vyhledávání pomocí protokolu SNMP (Simple Network Mail Protocol).	0 = Ne, 1 = Ano	Zaškrtávací okénko protokolu SNMP: Jak ověřit systémy

Následující tabulka obsahuje nastavení souboru vlastností (/Qibm/UserData/OS400/Mgtc/Config/McConfig.properties), která pravděpodobně budete muset změnit, abyste splnili požadavky systému. K provedení těchto změn použijte znakově orientované rozhraní, není-li uvedeno jinak.

Tabulka 4. Parametry souboru vlastností Centrální správy

Parametr	Popis	Hodnoty	
QYPS_SSL	Zapíná či vypíná vrstvu SSL (Secure Sockets Layer).	0 = vypnuto, 1 = zapnuto	Jméno pole v produktu iSeries Navigator **(klepněte pravým tlačítkem na Centrální správa → Vlastnosti → karta Zabezpečení)**, jméno pole = Používat SSL (Secure Sockets Layer)
QYPS_AUTH_LEVEL	Úroveň autentizace přes SSL. Tato hodnota pracuje s parametrem QYPS_SSL.	0 = vypnuto (Toto je předvolená hodnota. Lze se připojit pouze k serveru bez SSL.), 1 = zapnuta serverová autentizace (To znamená, že se lze připojit k serveru s či bez SSL.)	iSeries Navigator **(klepněte pravým tlačítkem na Centrální správa → Vlastnosti → karta Zabezpečení)**, jméno pole = Úroveň autentizace
QYPS_USER_PASSWORD	Vyžadovat heslo v koncových systémech.	0 = Ne, 1 = Ano	iSeries Navigator **(klepněte pravým tlačítkem na Centrální správa → Vlastnosti → karta Zabezpečení)**, jméno pole = Použít autentizaci uživatelského profilu a hesla
QYPSJ_SYSTEM_ID	Uživatelský profil, pod kterým se server Java spouští pro určité úlohy.	QSECOFR (Toto je předvolená hodnota.). Také můžete zadat jméno profilu, ten však musí mít třídu oprávnění *SECOFR.	

Přidání koncových systémů do sítě Centrální správy

Koncový systém je libovolný systém nebo logická část ve vaší síti TCP/IP, které chcete spravovat z vašeho centrálního systému.

Když přidáváte připojení k systému z prostředí produktu iSeries Navigator (klepnutím na položku **Soubor → Připojit k serverům → Přidat připojení**, přičemž v levém podokně je vybráno vaše aktuální prostředí), systém se přidá do seznamu pod vaším aktuálním aktivním prostředím (obvykle do položky Připojení). Když však přidáváte nový koncový systém, jméno systému se přidá do seznamu Koncové systémy v položce Centrální správa.

Když chcete provést akci v systému v položce Připojení, požaduje se přímé připojení od klienta (vaše PC) k příslušnému systému, a akce se v daném okamžiku provádějí na jednom systému. Na rozdíl od toho umožňuje Centrální správa provádět úlohy správy systémů na více systémech (v seznamu koncové systémy) a požaduje se pouze jedno klientské připojení (k centrálnímu systému).

Centrální systém obsluhuje jednotlivá připojení ke koncovým systémům. Nastavení vlastnosti Centrální správa pro Frekvenci vyhledávání řídí způsob určení IP adresy pro koncový systém. Je-li nastavena na hodnotu NIKDY, použije se IP adresa uložená v koncovém objektu. Je-li nastavena na hodnotu VŽDY, poskytne protokol TCP/IP na serveru IP adresu pro zadané jméno systému.

Poznámka: Jestliže přidáváte koncové systémy s operačním systémem OS/400 V5R1, musíte mít v systému V5R1 nainstalované tyto opravy (známé také jako PTF): SI01375, SI01376, SI01377, SI01378 a SI01838. Bez těchto souborů nebudete moci na koncovém systému používat všechny funkce pro správu systémů.

Chcete-li přidat jeden nebo více koncových systémů, postupujte takto:

1. Klepněte pravým tlačítkem myši na **Koncové systémy** a vyberte **Nový koncový systém**.
2. Zadejte jméno systému a klepněte na **OK**.

Koncové systémy, které přidáte, se automaticky objeví v položce **Koncové systémy** v okně produktu iSeries Navigator. Po přidání koncového systému můžete zobrazit jeho vlastnosti. Podle potřeby také můžete změnit popis IP adresy.

Dále můžete vytvořit skupiny systémů, které vám pomohou spravovat různé sady koncových systémů. Nové systémové skupiny se zobrazí v Centrální správě v okně produktu iSeries Navigator.

Další informace o těchto a jiných úlohách a tématech Centrální správy naleznete v podrobné nápovědě k úlohám, která je dostupná v prostředí produktu iSeries Navigator. Na řádkovém menu klepněte na **Nápověda** a vyberte **Přehled produktu iSeries Navigator → Centrální správa**.

Úplné odstranění koncových bodů

Toto téma odpovídá na otázku: Proč se koncový bod vymazaný z Centrální správy později znovu objeví?

Při připojování k cílovému systému Centrální správa vyžaduje a používá objekty koncových bodů. Kromě toho se mnoho funkcí Centrální správy objeví v systémech uvedených pod položkou Připojení. Kdykoli tak uživatel pod položkou Připojení vytvoří systém, dojde k uložení objektu koncového bodu do databáze v centrálním systému i v klientském počítači.

Při vymazání koncového bodu z Centrální správy dojde pouze k vymazání záznamu z databáze centrálního systému. Systém musíte také vymazat ze všech klientů, ve kterých je systém uveden pod položkou Připojení. Jinak bude uživateli, který má systém pod položkou Připojení stále uveden a který znovu spustí iSeries Navigator, automaticky opět přidán koncový bod do Centrální správy.

Chcete-li proto zcela odstranit koncový bod, který je definován jako systém položky Připojení, musí ho všichni uživatelé, kteří ho mají definovaný, odstranit z položky Připojení tak, aby nebyl automaticky přidáván.

Vytvoření skupin systémů v síti Centrální správy

Skupina systémů je kolekce koncových systémů, kterou definujete. Jestliže pracujete s více systémy nebo více logickými částmi, vytvoření skupin systémů vám umožní provádět úlohy ve všech těchto systémech, aniž byste vybírali každý koncový systém jednotlivě. Stačí jednoduše vybrat skupinu systémů, kterou jste vytvořili, a můžete začít s prováděním úlohy.

Koncové systémy mohou patřit do několika skupin systémů zároveň. Jakmile vytvoříte skupinu systémů, můžete spravovat celou skupinu z centrálního systému, jako by to byl jediný systém.

Při vytváření skupiny systémů postupujte takto:

1. V prostředí produktu **iSeries Navigator** vyhledejte a otevřete položku **Centrální správa**.
2. Klepněte pravým tlačítkem myši na **Skupiny systémů** a zvolte **Nová skupina systémů**.
3. V okně **Nová skupina systémů** uveďte jedinečné jméno nové skupiny systémů. Můžete zadat i stručný popis, který vám později pomůže skupinu rozpoznat na seznamu skupin systémů.
4. V seznamu **Dostupné systémy** vyberte koncové systémy, které chcete zahrnout do této nové skupiny. Klepnutím na tlačítko **Přidat** přidáte tyto systémy do seznamu **Vybrané systémy**.
5. Pokud chcete jiným uživatelům umožnit prohlížení nebo změnu této skupiny systémů, použijte sdílení. Klepněte na ouško **Sdílení** a uveďte **Pouze pro čtení** nebo **Úplné** sdílení. Pokud uvedete **Žádné**, jiní uživatelé si tuto skupinu systémů nebudou moci prohlížet ani měnit, pokud nebudou mít speciální oprávnění, které je spravováno v položce Hostitelské aplikace v Administrativě aplikací. Uživatelé s tímto speciálním oprávněním nazvaným Přístup k administrativě Centrální správy si mohou zobrazit všechny úlohy, definice, monitory a skupiny systémů v Centrální správě v okně iSeries Navigator.
6. Novou skupinu systémů vytvoříte klepnutím na **OK**.

Skupina systémů, kterou vytvoříte, bude zahrnovat všechny koncové systémy, které jste zadali. Tento seznam koncových systémů můžete později upravit. Do své skupiny můžete kdykoli přidat další koncové systémy nebo z ní koncové systémy odstranit.

Skupiny systémů můžete z Centrální správy vymazat. Když vymažete skupinu systémů nebo odstraníte koncové systémy ze skupiny systémů, změní se pouze daná skupina systémů. Koncové systémy, které byly ve skupině systémů, jsou stále uvedeny pod položkou **Koncové systémy** v okně produktu iSeries Navigator. Vymažete-li ze seznamu **Koncové systémy** určitý koncový systém, je tento systém odstraněn ze všech skupin systémů.

Další informace o těchto a jiných úlohách a tématech Centrální správy naleznete v podrobné nápovědě k úlohám, která je dostupná v prostředí produktu iSeries Navigator. Na řádkovém menu klepněte na **Nápověda** a vyberte **Přehled produktu iSeries Navigator → Centrální správa**.

Související informace

Centrální správa a Administrace aplikací

Změna nastavení centrálního systému

Jako centrální systém si můžete kdykoli zvolit jiný systém. Centrální systém musí být takový systém, k němuž jste přímo připojeni. Chcete-li používat nejnovější funkce produktu iSeries Navigator, musí být ve vašem centrálním systému spuštěn operační systém i5/OS verze 5, vydání 4 (V5R4).

Jestliže máte ve svém PC produkt iSeries Navigator verze V5R2 nebo V5R3 a chcete si vybrat centrální systém, ve kterém je spuštěn operační systém OS/400 V5R1, musíte mít v systému V5R1 instalované tyto opravy (známé také jako PTF): SI01375, SI01376, SI01377, SI01378 a SI01838. Bez těchto PTF nebudete schopni připojit se k systému s verzí V5R1 jako k centrálnímu systému.

Chcete-li změnit svůj centrální systém, postupujte takto:

1. Klepněte pravým tlačítkem myši na centrální správu a zvolte **Změnit centrální systém**.
2. V okně **Změnit centrální systém** si vyberte systém ze seznamu připojených systémů.
3. Pokud systém, který chcete použít jako centrální systém, není momentálně připojen do sítě produktu iSeries Navigator, klepněte pravým tlačítkem myši na aktivní prostředí (obvykle se jedná o Připojení) a vyberte volbu **Připojit k serverům → Přidat připojení**. Jakmile bude nový systém připojen, budete moci změnit centrální systém na nový systém.

Jakmile přidáte koncové systémy a vytvoříte skupiny systémů, tyto koncové systémy a skupiny systémů se objeví pod Centrální správou. Jakmile nastavíte centrální systém, můžete provést další nutné úlohy související s nastavením Centrální správy.

Důležité: Centrální systém, který používáte by měl být stejného nebo novějšího vydání než použité koncové systémy.

Další informace o těchto a jiných úlohách a tématech Centrální správy naleznete v podrobné nápovědě k úlohám, která je dostupná v prostředí produktu iSeries Navigator. Na řádkovém menu klepněte na **Nápověda** a vyberte **Přehled produktu iSeries Navigator → Centrální správa**.

Odstraňování problémů s připojením Centrální správy

Připojení k Centrální správě může zabránit několik faktorů. Toto téma obsahuje seznam kroků sloužících k odstranění problémů se selhaným připojením.

Nejprve se ujistěte, že v centrálním systému je spuštěno nejvyšší vydání operačního systému v síti. Problémy mohou být způsobeny tím, že v síti jsou klienti, ve kterých je spuštěn operační systém s novějším vydáním než centrální systém.

Související informace

Scénář: Zabezpečení všech připojení k serveru Centrální správy pomocí vrstvy SSL

Zpráva o zkušenosti: Configuring Management Central Connections for Firewall Environments

Produkt Digital Certificate Manager

Selhané připojení k centrálnímu systému

1. Z PC ověřte, zda je pomocí jména nebo IP adresy uvedené v produktu iSeries Navigator pro centrální systém možné spustit příkaz ping na centrální systém. Je-li příkaz neúspěšný, je problém v síti nebo DNS či tabulce hostitelů. Před pokračováním musíte tento problém odstranit.
2. Ujistěte se, že pomocí IP adresy daného PC lze z centrálního systému spustit příkaz ping na PC. Není-li tento příkaz úspěšný, nebudete moci používat některé funkce Centrální správy. Další informace naleznete ve zprávě o zkušenosti v aplikaci Information Center: Configuring Management Central Connections for Firewall Environments.
3. Ověřte připojení centrálního systému. (V prostředí produktu iSeries Navigator rozbalte položku **Připojení → klepněte pravým tlačítkem na server, který je centrálním systémem → Ověřit připojení**.) Pokud tento postup ohlásí chyby, klepněte na volbu **Podrobnosti**. Zobrazí se okno obsahující informace o tom, k čemu došlo.
4. K dalšímu odstranění problémů použijte funkci Ověřit připojení v Centrální správě. (V prostředí produktu iSeries Navigator klepněte pravým tlačítkem na **Centrální správa → Ověřit připojení**.) Pokud tento postup ohlásí chyby, klepněte na volbu **Podrobnosti**. Zobrazí se okno obsahující informace o tom, k čemu došlo.

Co dělat, pokud připojení stále nefunguje

Pokud připojení stále nefunguje, použijte k dalšímu odstranění problémů tento postup:

1. Ověřte, zda je v centrálním systému spuštěn server Centrální správy QYPSJSVR.
   a. V prostředí produktu iSeries Navigator rozbalte **Připojení → server, který používáte jako centrální systém → Síť → Servery → TCP/IP**.
   b. V položce Centrální správa zkontrolujte, zda je server spuštěn. V případě potřeby klepněte pravým tlačítkem na Centrální správu pod položkou TCP/IP a klepněte na volbu **Spustit**.
   c. Pokud se server stále nedaří spustit, zkontrolujte, zda v protokolech úloh nejsou zaznamenány nějaké problémy, nebo pomocí dalších kroků ověřte, zda nenastaly některé běžné problémy způsobující, že servery se nemohou spustit.
2. Zkontrolujte konfiguraci protokolu TCP/IP v centrálním systému.
   a. Centrální systém musí být schopen spustit příkaz ping sám na sebe ať už pomocí plně kvalifikovaného jména domény, nebo pomocí krátkého jména. Pokud se příkaz ping na jedno z těchto jmen nezdaří, budete muset toto jméno a IP adresu přidat buď do systémové tabulky hostitelů nebo DNS. Ujistěte se, že IP adresa použitá v těchto příkazech ping je ta, kterou PC může kontaktovat.
3. Pokud s Centrální správou používáte vrstvu zabezpečení SSL, ověřte, že je nastavena správně. Musíte v PC nakonfigurovat Centrální správu, všechny koncové systém i produkt iSeries Navigator.
4. Zkontrolujte profil QSECOFR.
   a. Centrální správa vyžaduje profil s povolenými oprávněními *ALLOBJ a *SECOFR. Dále musí být nastaveno platné heslo tak, aby nevypršela jeho platnost.

      Důležité: Tuto změnu musíte provést ve znakově orientovaném rozhraní, jinak server nemusí soubor přečíst.

      V předvoleném nastavení Centrální správa používá profil QSECOFR. Pokud tedy toto předvolené nastavení nebylo změněno, můžete povolit profil QSECOFR a heslo nastavit tak, aby nikdy nevypršela jeho platnost. (Pokud heslo nenastavíte tak, aby jeho platnost nikdy nevypršela, musíte pečlivě dbát na to, aby bylo stále aktivní. Toho docílíte tak, že vždy **před** vypršením jeho platnosti heslo změníte.) Používáte-li přizpůsobený profil (jiný než QSECOFR), povolte ho a heslo nastavte tak, aby jeho platnosti nikdy nevypršela. Chcete-li změnit profil QSECOFR, otevřete soubor vlastností ″/QIBM/UserData/OS400/MGTC/config/McConfig.properties″. Změňte parametr ″QYPSJ_SYSTEM_ID = QSECOFR″ na ″QYPSJ_SYSTEM_ID = VÁŠ_PROFIL″ (kde VÁŠ_PROFIL je profil nahrazující profil QSECOFR).
   b. Nebo můžete spustit příkaz

      ```
      CALL PGM(QSYS/QYPSCONFIG) PARM(xxxx 'yyyy')
      ```

      kde xxxx je QYPSJ_SYSTEM_ID a yyyy je jméno profilu, který se má použít.

5. Pokud jsou v centrálním systému úspěšně spuštěny oba servery Centrální správy a pokud jste odstranili problémy podle výše uvedeného postupu a stále se nedaří připojit z produktu iSeries Navigator, pak je nejpravděpodobnějším problémem konfigurace související s TCP/IP nebo ochrannou bariérou. V obou případech k odstranění problému použijte zprávu o zkušenosti Configuring Management Central Connections for Firewall Environments. Níže je uvedeno několik důležitých poznámek:
   - Centrální systém musí být schopen iniciovat připojení k produktu iSeries Navigator v PC. Proto je důležité, aby centrální systém mohl úspěšně spustit příkaz ping na IP adresu PC.
   - PC musí být schopno iniciovat připojení k produktu iSeries Navigator, který používá následující IP adresy:
     – Jméno nebo IP adresa používaná jako jméno centrálního systému v prostředí produktu iSeries Navigator (jméno systému pod položkou Připojení).
     – IP adresa, kterou centrální systém získá, když spustí příkaz ping sám na sebe.

     Poznámka: Výchozí připojení k centrálnímu systému používá jméno nebo IP adresu zadanou v produktu iSeries Navigator pro centrální systém. Během tohoto výchozího připojení však centrální systém zjistí vlastní IP adresu a odešle ji do PC. PC tuto IP adresu použije pro všechna další připojení. Porty, které Centrální správa používá, musí být ve všech používaných ochranných bariérách otevřené.

Selhané připojení z PC do centrálního systému

1. Klepněte pravým tlačítkem myši na Centrální správu a spusťte Ověření připojení.
2. Ujistěte se, že pro servery Centrální správy je zapnuta vrstva SSL (single socket layer). V souboru /qibm/userdata/os400/mgtc/config/McConfig.properties se přesvědčete, že hodnota QYPS_SSL > 1 nebo hodnota QYPS_AUTH_LEVEL > 1. Pokud tyto hodnoty změníte, musíte servery Centrální správy restartovat.
3. Selhalo spuštění úlohy QYPSSRV v případě, že používáte operační systém OS/400 V5R2? Pokud spuštění selhalo, nebyla konfigurace správce DCM (Digital Certificate Manager) provedena správně. Ujistěte se, že jste svému certifikátu přiřadili identifikaci aplikace Centrální správa a ID hostitelského serveru.
4. Je vedle centrálního systému ikona visacího zámku? Pokud není, pak klient k připojení nepoužívá vrstvu SSL. Pod položkou Připojení klepněte pravým tlačítkem na centrální systém, přejděte na kartu SSL a zvolte použití vrstvy SSL. Pak klepněte na **OK**. Nastavení se projeví až po zavření a restartování produktu iSeries Navigator.
5. Na stejné kartě SSL (zmíněné v kroku 3) se nachází tlačítko pro stažení CA do PC. Ujistěte se, že jste stažení provedli pomocí operačního systému, na kterém jste CA VYTVOŘILI (nemusí to být nezbytně centrální systém).
6. Na stejné kartě SSL zmíněné v předchozím odstavci se nachází volba Ověřit připojení SSL. Spusťte ji a prohlédněte si výsledky.
7. Používáte-li operační systém OS/400 V5R2, ověřte, že v souboru QIBM\ProdData\OS400\Java400\jdk\lib\security\java.security jsou definovány následující vlastnosti, protože ty mohou způsobit problémy s připojením.
   - os400.jdk13.jst.factories=true
   - ssl.SocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLSocketFactoryImpl
8. Používáte-li v klientovi operační systém OS/400 V5R2, podívejte se v PC na soubor c:\Documents and Settings\All Users\Documents\ibm\client access\classes\com\ibm\as400\access\KeyRing.class. Má velikost 0? Pokud ano, smažte ho a stáhněte si vydavatele certifikátů (CA).

Selhané připojení z centrálního systému do koncového systému

Kromě provedení následujícího postupu odstraňování problémů se selhaným připojením z PC do centrálního systému byste si také měli prohlédnout protokol úlohy v centrálním systému. Tam byste měli najít důvod, proč bylo připojení zamítnuto. (Například: (CPFB918) Připojení k systému mysystem.mydomain.com bylo zamítnuto. Úroveň autentizace 0. Kód příčiny 99. To znamená, že pro koncový systém není aktivní vrstva SSL. Namísto toho je autentizace na úrovni 0.) Významy negativních kódů příčin můžete najít v souboru /QSYS.LIB/QSYSINC.LIB/H.FILE/SSL.MBR.

Poznámka: Koncové systémy nevyžadují zámek.

Další otázky

Otázky týkající se ochranné bariéry

Veškerá komunikace TCP je inicializována z PC k centrálnímu systému. Přidáním následujícího řádku do souboru C:\MgmtCtrl.properties můžete zadat konkrétní port, který se má použít:

```
QYPSJ_LOCAL_PORT=xxxx
```

kde xxxx je číslo portu. Číslo portu by mělo být větší než 1024 a menší než 65535. Kromě toho toto číslo portu nesmí používat jiná aplikace v PC. Port musí být otevřený přes ochrannou bariéru. Pokud to ochranná bariéra vyžaduje, musí být otevřeny všechny sokety.

Práce s Centrální správou

Centrální správu můžete po jejím nastavení použít k zefektivnění úloh správy.

Prohlášení o licenci a vyloučení záruky pro příklady programovacího kódu

Společnost IBM vám uděluje nevýhradní licenci na užívání všech příkladů programovacího kódu, ze kterých můžete generovat podobnou funkci přizpůsobenou vašim konkrétním potřebám.

| KROMĚ JAKÝCHKOLI ZÁKONNÝCH ZÁRUK, KTERÉ NEMOHOU BÝT VYLOUČENY, IBM, JEJÍ
| PROGRAMOVÍ VÝVOJÁŘI A DODAVATELÉ NEPOSKYTUJÍ ZÁRUKY ANI PODMÍNKY, VYJÁDŘENÉ
| NEBO ODVOZENÉ, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI NEBO VHODNOSTI
| PRO URČITÝ ÚČEL A ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN V SOUVISLOSTI S PROGRAMEM
| NEBO TECHNICKOU PODPOROU, POKUD EXISTUJE.

| ZA ŽÁDNÝCH OKOLNOSTÍ NEJSOU IBM, JEJÍ PROGRAMOVÍ VÝVOJÁŘI NEBO DODAVATELÉ
| ODPOVĚDNI ZA ŽÁDNOU Z NÍŽE UVEDENÝCH SITUACÍ, ANI V PŘÍPADĚ, ŽE BYLI O MOŽNOSTI JEJICH
| VZNIKU PŘEDEM INFORMOVÁNI:

| 1. ZTRÁTA NEBO POŠKOZENÍ DAT;
| 2. PŘÍMÉ, ZVLÁŠTNÍ, NAHODILÉ NEBO NEPŘÍMÉ ŠKODY, NEBO LIBOVOLNÉ NÁSLEDNÉ
| EKONOMICKÉ ŠKODY; NEBO
| 3. ZTRÁTA ZISKU, OBCHODNÍHO OBRATU, PŘÍJMŮ, DOBRÉHO JMÉNA NEBO PŘEDPOKLÁDANÝCH
| ÚSPOR.

| PRÁVNÍ ŘÁDY NĚKTERÝCH ZEMÍ NEPŘIPOUŠTĚJÍ VYLOUČENÍ NEBO OMEZENÍ PŘÍMÝCH,
| NAHODILÝCH NEBO ODVOZENÝCH ŠKOD, A PROTO SE NA VÁS NĚKTERÁ NEBO VŠECHNA VÝŠE
| UVEDENÁ OMEZENÍ NEBO VYLOUČENÍ NEMUSÍ VZTAHOVAT.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

Společnost IBM nemusí v ostatních zemích nabídnout produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použít lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu 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 zaslat 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 vaší zemi, nebo písemně zastoupení společnosti IBM na adrese:

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

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, MIMO JINÉ, ODVOZENÝCH ZÁRUK PORUŠENÍ ZÁKONŮ, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk 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 produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány 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 distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoli závazků 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 těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na programy, v Licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Veškerá data obsažená v tomto dokumentu byla získána v řízeném prostředí. Výsledky získané v jiném provozním prostředí se tudíž mohou výrazně lišit. Některá měření byla provedena v systémech s vývojovým prostředím a neexistuje žádná záruka, že tato měření budou stejná v obecně dostupných systémech. Některá měření byla odhadnuta extrapolací. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit vhodnost dat pro svá specifická prostředí.

Informace týkající se jiných produktů než od IBM byly získány od dodavatelů těchto produktů, jejich zveřejněných prohlášení a jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy na možnosti produktů pocházejících z jiného zdroje než od IBM adresujte dodavatelům těchto produktů.

Veškerá prohlášení, týkající budoucích trendů nebo strategií IBM, podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

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:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyku, které ilustrují programovací metody na různých operačních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Tyto vzorové programy nebyly důkladně testovány za všech podmínek. IBM proto nezaručuje ani nenaznačuje spolehlivost, provozuschopnost a funkčnost těchto programů.

Každá kopie nebo část těchto vzorových programů nebo jakákoliv odvozená práce musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů. © 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.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:

AIX
AIX 5L
e(logo)server
eServer
i5/OS
IBM

| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (loga), MMX Pentium jsou ochranné známky společnosti Intel Corporation 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

| Linux je ochranná známka Linus Torvalds ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka společnosti Open Group ve Spojených státech a případně v dalších jiných zemích.

Názvy jiných společností, produktů a služeb mohou být ochrannými nebo servisními známkami jiných společností.

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 NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.

Vytištěno v Dánsku společností IBM Danmark A/S.