KAPITOLA

9

Konfigurace a správa řízení přístupu v systému VMware vSphere

Témata kapitoly:

- **Správa a údržba povolení hostitelů ESX/ESXi**
- **Správa a údržba povolení systému vCenter Server**
- **Správa virtuálních strojů pomocí webové konzoly**
- **Cvičení**

Centralizace správy virtuálních strojů a jejich hostitelů ESX/ESXi se stala problémem ve většině rostoucích datových centrech. Důležitou částí centralizovaného modelu správy je předání řízení příslušným uživatelům, aby se mohli podílet na správě virtuální infrastruktury. Jak třeba přidělíte povolení uživatelům, kteří nastavují virtuální stroje pro testování nové aplikace? Měli by mít možnost vytvářet virtuální stroj a řídit přístup k prostředkům, ale současně by měli být omezeni v jiných oblastech virtuální infrastruktury.

Povolení k virtuální infrastruktuře můžete spravovat systémem vCenter Server nebo přímo hostitelem ESX/ESXi.

V této kapitole se naučíte:

- Spravovat a udržovat povolení hostitelů ESX/ESXi.
- Spravovat a udržovat povolení systému vCenter Server.
- Spravovat virtuální stroje pomocí webové konzoly.

Správa a údržba povolení hostitelů ESX/ESXi

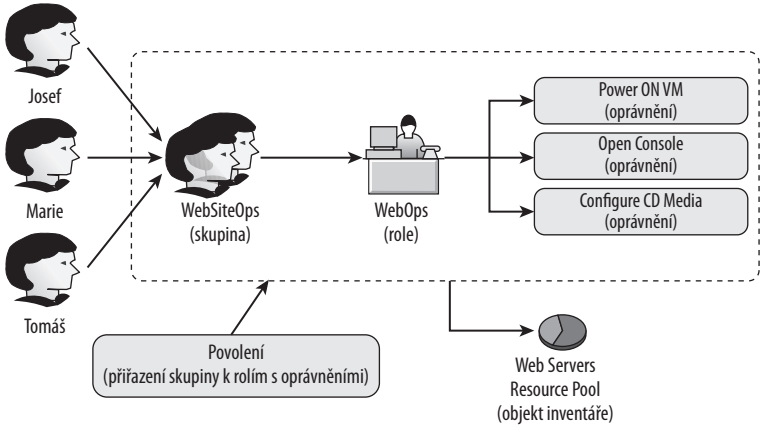
Systém vCenter Server i hostitelé ESX/ESXi používají stejný model zabezpečení, podle kterého umožňují uživatelům spravovat části virtuální infrastruktury. Tento model se skládá z uživatelů, skupin, rolí, práv a povolení, jak ukazuje obrázek 9.1.

Prostředí systému vCenter Server se od jiných prostředí liší hlavně ve dvou oblastech:

- Vyhledávání vytvořených objektů uživatelů a skupin.
- Úroveň granularity rolí a práv v každém prostředí.

V prostředí bez systému vCenter Server, nebo kde správce rozhodl, že uživatelé se musí přihlásit přímo k hostitelům ESX/ESXi, je důležité, abyste začali diskuzí o modelu zabezpečení.

Povolení k hostitelům ESX/ESXi jsou přidělována přímo uživatelům a skupinám na určitém hostiteli.



Obrázek 9.1: Systém vCenter Server a hostitelé ESX/ESXi mají stejný model zabezpečení pro řízení přístupu

Uživatele a skupiny hostitele ESX/ESXi zobrazíte následovně:

1. Spusťte klienta vSphere Client a připojte se k hostiteli ESX/ESXi.
2. Zobrazte inventář **Hosts And Clusters** výběrem položky **View → Inventory → Hosts And Clusters** z nabídky. Rovněž můžete použít navigační panel nebo klávesovou zkratku **Ctrl+Shift+H**.
3. Vyberte hostitele ESX/ESXi ve stromě inventáře nalevo a potom klepněte na záložku **Users & Groups** v podokně napravo.

Když budujete virtuální infrastrukturu, je z bezpečnostního hlediska důležité zjistit, kdo ve vaší společnosti musí přistupovat k hostiteli ESX/ESXi, ať už pomocí spojení SSH (například pomocí programů PuTTY, WinSCP, FastSCP atd.), klienta vSphere Client, nebo webového rozhraní, které budu popisovat dále v této kapitole (v části *Správa virtuálních strojů pomocí webové konzoly*). Uživatelské jméno a heslo k účtu root byste měli šířit opatrně. Pokud bude muset více uživatelů přistupovat přímo k hostiteli ESX/ESXi, dejte každému uživateli samostatný účet.

> **NĚKTERÉ NÁSTROJE NELZE POUŽÍT S HOSTITELEM ESXI**
>
> Ačkoliv hostitel VMware ESX i hostitel VMware ESXi spravují a ukládají uživatele a skupiny lokálně, chybějící konzolový systém v hostiteli ESXi znamená, že nástroje typu PuTTy, WinSCP, FastSCP atd. nelze použít s hostitelem ESXi. Hostitele ESXi je možné plně spravovat jen pomocí klienta vSphere Client.

Jak bylo řečeno na začátku kapitoly, model zabezpečení systému vCenter Server a hostitelů ESX/ESXi se skládá z uživatelů, skupin, rolí, práv a povolení. V základní verzi modelu zabezpečení jsou uživatelé nebo skupiny přidělené k rolím, které mají práva. Kombinace uživatel-role-právo je potom spojena s objektem v inventáři jako povolení.

Pod záložkou **Users & Groups** najdete dvě tlačítka – tlačítko **Users** a tlačítko **Groups**. Zde můžete přiřazovat uživatele a skupiny k příslušným rolím. Co to přesně je *role*?

Povolení hostitele ESX/ESXi mají zjednodušit přiřazování. Místo toho, abyste práva přiřazovali jednotlivě, přiřadíte uživatele nebo skupinu k roli. Hostitel ESX/ESXi má tři výchozí role – No Access, Read-Only a Administrator.

Přestože jsou významy těchto rolí poměrně zřejmé, podívejme se na každou z nich:

No Access: tato role brání přistupovat k objektům v inventáři. Roli No Access je možné použít, pokud má uživatel přístup k vyšším objektům inventáře. Roli No Access lze také použít na objekty na nízké úrovni, abyste zabránili přístupu k objektům. Jestliže jsou například uživateli přiřazena povolení na hostiteli ESX/ESXi, ale neměl by mít přístup k určitému virtuálnímu stroji, mohli byste na tomto stroji použít roli No Access.

Read-Only: role Read-Only umožňuje uživateli prohlížet objekty v inventáři klienta vSphere Client. Nijak neumožňuje uživateli zasahovat do viditelných objektů. Například uživatel s rolí Read-Only by viděl seznam virtuálních strojů inventáře, ale nemohl by na nich nic dělat.

Administrator: role Administrator má nejvyšší oprávnění, ale je to pouze role, kterou musíte přiřadit kombinaci objektu uživatele nebo skupiny a objektu inventáře, například virtuálnímu stroji.

Se třemi rolemi na hostitelích ESX/ESXi nezbývá příliš prostoru pro flexibilitu. Ale zbytečně nezoufejte – omezení dané výchozími rolemi se rychle ztratí díky možnosti vytvářet vlastní role. Můžete vytvářet vlastní role, které lépe splní vaše požadavky, případně můžete zkopírovat existující roli a upravit ji podle vlastních představ.

Neměli byste upravovat přímo výchozí role. Pokud vám role nevyhovuje, vytvořte si vlastní. Jestliže změníte výchozí roli, riskujete, že nějaký správce přidělí uživatelům příliš mnoho nebo příliš málo povolení, protože je přiřadí k výchozí roli.

O vytváření vlastních rolí už toho bylo řečeno dost, pojďme se podívat, jak to udělat.

VÝCHOZÍ PŘIŘAZENÍ POVOLENÍ NA HOSTITELÍCH ESX/ESXI

Když nainstalujete hostitele ESX/ESXi, existuje na něm pouze uživatel root a tento uživatel má všechna povolení k celému serveru. Tato výchozí sada povolení se změní, pokud spravujete hostitele ESX/ESXi systémem vCenter Server. Proces přidání hostitele do systému vCenter Server přidá agenta (agent vCenter Server Agent) a další účet s názvem vpxuser. Účet vpxuser má 32znakové náhodně generované heslo a také je mu přiřazena role Administrator na hostiteli ESX/ESXi. Díky tomu může služba vCenter Server provádět úlohy na hostitelích ESX/ESXi.

Vytváření vlastních rolí

Pokud výchozí role hostitele ESX/ESXi nevyhovují potřebám vaší organizace, měli byste vytvořit vlastní role. Předpokládejme třeba, že někteří uživatelé musí pracovat s konzolou na virtuálním stroji a také potřebují měnit vyměnitelná média na těchto virtuálních strojích. Těmto požadavkům nevyhovuje ani jedna výchozí role, takže je nutná nová role.

Následujícím postupem vytvoříte vlastní roli s názvem Operator:

1. Spusťte klienta vSphere Client a připojte se k hostiteli ESX/ESXi.

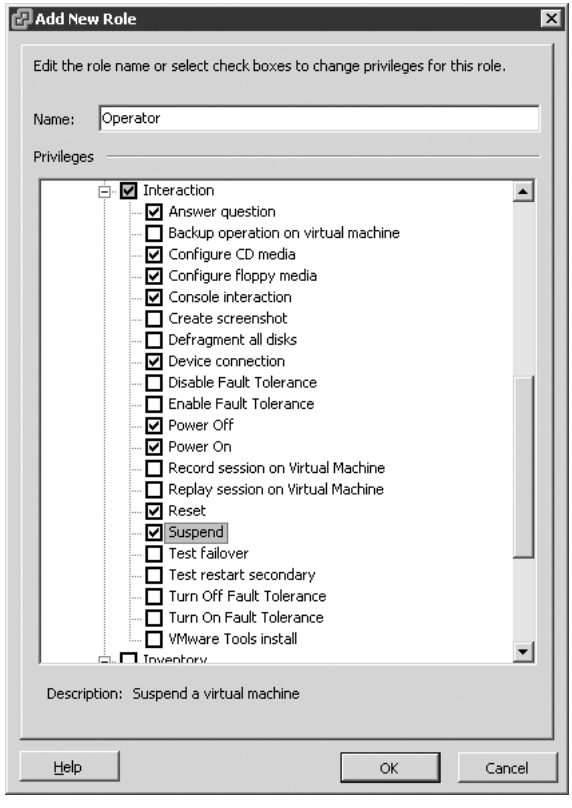
2. Přejděte do oblasti Administration prostřednictvím navigačního panelu nebo výběrem položky **View → Adminstration → Roles**. Můžete rovněž použít klávesovou zkratku **Ctrl+Shift+R**.
3. Klepněte na tlačítko **Add Role**.
4. Zadejte název nové role do textového pole **Name** (v tomto případě Operator) a potom vyberte práva, která budou mít členové role, jak vidíte na obrázku 9.2.

   Práva z obrázku 9.2 umožňují uživatelům a skupinám přiřazeným roli Operator pracovat s konzolou virtuálního stroje, měnit vyměnitelná média a vypínat a zapínat virtuální stroj.

POVOLENÍ PRO ZMĚNU VIRTUÁLNÍCH MÉDIÍ

Abyste mohli vyměnit disketu nebo kompaktní disk pomocí obrazu diskety (soubor s příponou **.flp**) nebo obrazu disku CD/DVD (soubor s příponou **.iso**), které jsou uloženy na jednotce SAN, musíte mít skupinu práv Browse Datastore v kořenu hierarchie – v tomto případě na samotném hostiteli ESX/ESXi.

5. Klepnutím na tlačítko **OK** vytvoříte vlastní roli.



Obrázek 9.2: Vlastní role posilují schopnosti správy a přidávají flexibilitu k přidělování povolení

Nyní jste vytvořili novou roli Operator, ale ještě není funkční. Musíte ještě k roli přiřadit uživatele nebo skupiny a aplikovat roli na hostitele ESX/ESXi nebo virtuální stroj

Přidělování povolení

Ať už jsou role jakkoliv užitečné, nefungují, dokud k nim nepřiřadíte uživatele nebo skupinu a potom je nepřiřadíte objektu inventáře. Předpokládejme, že existuje skupina uživatelů, kteří musí komunikovat se všemi virtuálními stroji typu webový server. Pokud spravujete přístup na hostiteli ESX/ESXi, musíte vytvořit na tomto hostiteli uživatelský účet a skupinu – například WebSiteOps. Až vytvoříte lokální uživatele nebo skupiny, můžete aplikovat tento model zabezpečení.

Právo na virtuálním stroji přidělíte lokálnímu uživateli nebo skupině následovně:

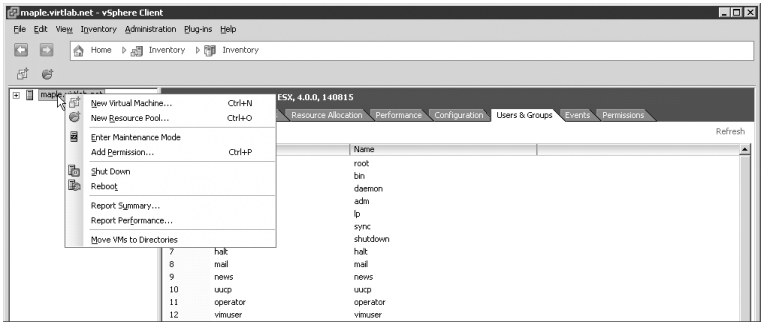
1. Spusťte klienta vSphere Client a připojte se k hostiteli ESX/ESXi.
2. Klepněte pravým tlačítkem myši na objekt, kterému chcete přiřadit povolení, ve stromu inventáře vlevo. Potom vyberte položku **Add Permision**. V tomto případě klepněte pravým tlačítkem myši na hostitele ESX/ESXi.
3. Klepněte na tlačítko **Add** v dialogovém okně **Assign Permissions**.
4. V dialogovém okně **Select Users And Groups** vyberte vhodného uživatele nebo skupinu (v tomto případě WebSiteOps), klepněte na tlačítko **Add** a potom na tlačítko **OK**. Tím otevřete dialogové okno **Assign Permissions**, kde jsou vlevo zobrazeni uživatelé a skupiny.
5. Z rozevíracího seznamu **Assigned Role** vyberte roli, ke které chcete uživatele nebo skupiny přiřadit. V tomto případě vyberte z rozevíracího seznamu dříve definovanou skupinu Operator, tím k ní přiřadíte skupinu WebSiteOps.

Co když budete mít hostitele ESX/ESXi s 30 virtuálními stroji a 10 z nich budou virtuální stroje webových serverů? Jak jste viděli dříve, musíte přiřadit povolení na každém z 10 virtuálních strojů webových serverů. Toto samozřejmě není efektivní přístup. Rostoucí počet webových serverů by vyžadoval více práce na zajištění řízení přístupu. Když vytvářítе roli, můžete si všimnout položky **Propagace To Child Objects**, která vám může usnadnit implementaci řízení přístupu.

Tato položka funguje stejně jako dědičná nastavení souborového systému v systémech Windows. Umožňuje přenést práva této role na objekty pod vybraným objektem. Když třeba přiřadíte roli Operator hostiteli ESX/ESXi v inventáři a povolíte možnost **Propagate To Child Objects**, všichni členové role Operator budou moci komunikovat se všemi virtuálními stroji hostitele ESX/ESXi. Přestože to zjednodušuje implementaci řízení přístupu, přidává to další problém – povolení. Role Operator byla přetížena a nyní platí pro všechny virtuální stroje, ne jen pro webové servery. Když máte povolení na úrovni hostitele, členové role Operator budou moci měnit vyměnitelná média a používat konzolu na virtuálních strojích webových serverů, ale to stejné budou moci provádět i na jiných typech virtuálních strojů v inventáři.

Tento problém přináší nevýhody při správě řízení přístupu na jednotlivých hostitelích ESX/ESXi. Nezapomínejte také, že všechny dosud představené postupy se týkaly jednotlivých hostitelů ESX/ESXi ve virtuální infrastruktuře. Co když by bylo možné nějak uspořádat inventář virtuálních strojů? Jinými slovy – co když byste mohli vytvořit „obalující objekt" pro všechny virtuální stroje webových serverů a umístit do něj všechny tyto virtuální stroje? Potom byste mohli přiřadit skupinu k roli na úrovni rodičovského objektu a nechat dědičnost, aby udělala svou práci.

Jak ukazuje obrázek 9.3, problém je v tom, že objekty složek nemůžou být na jediném hostiteli ESX/ESXi. To znamená, že vaší jedinou šancí je společná oblast prostředků.



Obrázek 9.3: Objekty složek nelze přidávat k jednotlivým hostitelům ESX/ESXi, poslední možnost tedy představuje společná oblast prostředků

Přiřazování povolení pomocí společné oblasti prostředků

Společná oblast prostředků je speciální objekt, který bude podrobněji popisovat příští kapitola, ale dobrá zpráva je, že zde vám může pomoci uspořádat vaše virtuální stroje. Výhodou společné oblasti prostředků je, že umí spravovat více virtuálních strojů jako objektů uvnitř logického objektu společné oblasti prostředků.

Následujícím postupem vytvoříte společnou oblast prostředků:

1. Spusťte klienta vSphere klient a připojte se k hostiteli ESX/ESXi.
2. Zobrazte pohled **Inventory** pomocí navigačního panelu, klávesové zkratky **Ctrl+Shift+H** nebo položky nabídky **View → Inventory → Inventory**.
3. Klepněte pravým tlačítkem myši na hostitele ESX/ESXi a vyberte položku **New Resource Pool**, jak jste viděli na obrázku 9.3.
4. Zadejte název společné oblasti prostředků do textového pole **Name**, v tomto případě zadejte název WebServers.
5. Jestliže to bude nutné, nastavte omezení a rezervace společné oblasti prostředků. Omezení zavede pevný limit pro využití prostředků, zatímco rezervace zavede garanci prostředků.

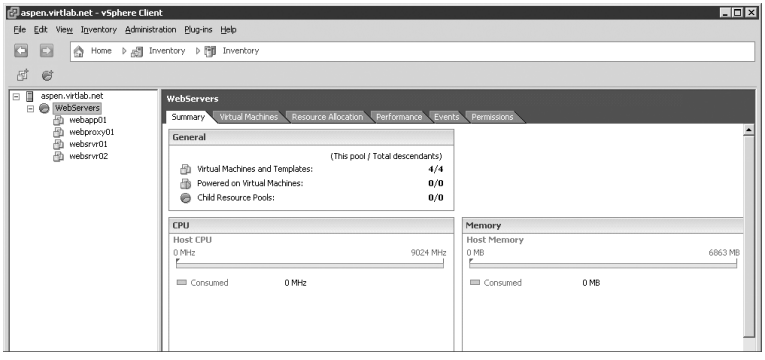
   O alokaci prostředků bude podrobněji pojednávat kapitola 10, „Správa alokace prostředků“.
6. Klepněte na tlačítko **OK**.

Když jste vytvořili společnou oblast prostředků WebServers, můžete do ní umístit virtuální stroje, jak ukazuje obrázek 9.4.

Ze společných oblastí prostředků se navíc stávají objekty inventáře, kterým je možné přiřazovat povolení. Zde platí stejný princip popsaný dříve v této kapitole, v části „Přidělování povolení“. Jednoduše přiřaďte povolení ke společné oblasti prostředků a zaškrtněte políčko **Propagate To Child Object**. Tato povolení pak budou platit pro všechny virtuální stroje ve společné oblasti prostředků.

Používání společné oblasti prostředků vám pomáhá dosáhnout několika cílů – lepší organizace virtuálních strojů a lepší kontroly nad povoleními přiřazenými těmto virtuálním strojům.

Ukázal jsem vám, jak přiřazovat povolení, ale co když budete chtít povolení odstranit? Odpověď najdete v následující části kapitoly.



Obrázek 9.4: Společné oblasti prostředků jsou jako objekty inventáře potenciálními úrovněmi správy infrastruktury

Odstranění povolení

Pokud musíte změnit správu nebo jste přiřadili práva špatně, můžete povolení odstranit. V části „Přidělování povolení" jste se dozvěděli, jak přiřadit povolení role Operators na hostiteli ESX/ESXi. Protože teď máte k dispozici skupinu prostředků, můžete odstranit povolení dříve přiřazená hostiteli.

Následujícím postupem odeberete povolení objektu inventáře:

1. Spusťte klienta vSphere klient a připojte se k hostiteli ESX/ESXi.
2. Zobrazte pohled **Inventory** prostřednictvím navigačního panelu, nabídky nebo klávesové zkratky.
3. Vyberte objekt inventáře a potom zvolte záložku **Permissions**. V tomto případě chcete odstranit povolení z hostitele ESX/ESXi, proto vyberte daného hostitele z inventáře.
4. Klepněte pravým tlačítkem myši na položku povolení, které chcete odstranit ze seznamu povolení, a potom vyberte položku **Delete**.

Měli byste uvidět varování, že uživatelé by si měli ponechat svá povolení, protože je mají přiřazena výše v hierarchii; v tomto případě je to však přesně to, čeho chcete dosáhnout. Chcete umožnit uživatelům přístup k virtuálním strojům na základě povolení přiřazených společné oblasti prostředků, a ne hostiteli ESX/ESXi.

Jakmile přiřadíte povolení přes inventář, je jednoduché ztratit přehled o tom, co jste udělali dříve. Samozřejmě, pokud vaše společnost nařizuje tvorbu dokumentace, možná máte k dispozici slušný revizní záznam. Lze však jednoduše prozkoumat využití současných rolí z klienta vSphere Client.

Identifikace použitých povolení

Jak roste inventář virtuálních strojů a společných oblastí prostředků, je velmi pravděpodobné, že se rovněž povolení přidělená různým objektům stanou složitější. Kromě toho – jak se postupně

mění potřeby společnosti a strategie správy, musí se měnit i tato povolení. Kombinací těchto faktorů může vzniknout prostředí, kde jsou povolení použita složitě a lze je těžko sledovat.

V boji s tímto problémem vám může pomoci pohled **Roles** klienta vSphere Client, kde můžete poznat, kde jsou přiděleny role a jak byla udělena povolení v inventáři.

Následující postup odhalí, kde byly role přiděleny jako povolení:

1. Spusťte klienta vSphere Client a připojte se k hostiteli ESX/ESXi.
2. Přepněte se na pohled **Roles** pomocí navigačního panelu, klávesové zkratky **Ctrl+Shift+R** nebo položky **View → Administration → Roles**.
3. Klepněte na roli, jejíž využití chcete sledovat.

V podokně detailů uvidíte, kde je role použita v hierarchii inventáře.

Pohled **Roles** klienta vSphere Client vám umožňuje sledovat, kde byla povolení přiřazena, abyste je mohli upravit nebo odstranit. Někdy však nestačí odstranit jen povolení a musíte odstranit i role.

Úprava a odstranění rolí

Je téměř nevyhnutelné, že se časem změní požadavky na správu. Až ten čas přijde, můžete vytvořit nové role, editovat současné role nebo dokonce smazat roli. Pokud už nelze použít ve vašem prostředí práva přiřazená roli, měli byste upravit roli a přidat do ní nebo z ní odebrat některá práva.

Roli upravíte následovně:

1. Spusťte klienta vSphere Client a připojte se k hostiteli ESX/ESXi.
2. Zobrazte pohled **Roles** prostřednictvím navigačního panelu, nabídky nebo klávesové zkratky.
3. Klepněte na roli, kterou chcete upravit, pravým tlačítkem myši a vyberte položku **Edit Role**.
4. V dialogovém okně **Edit Role** libovolně přidávejte nebo odstraňujte práva. Až budete hotovi, klepněte na tlačítko **OK**.

Nezapomeňte, že hostitel ESX/ESXi vám neumožní editovat výchozí role.

Pokud už roli nebudete potřebovat, měli byste ji odstranit, abyste snížili počet objektů, které musíte spravovat.

Následujícím postupem odstraníte roli:

1. Spusťte klienta vSphere Client a připojte se k hostiteli ESX/ESXi.
2. Zobrazte pohled **Roles** pomocí navigačního panelu, klávesové zkratky **Ctrl+Shift+R** nebo položky nabídky **View → Administration → Roles**.
3. Klepněte pravým tlačítkem myši na roli ke smazání a vyberte položku **Remove**.

Jestliže je vybraná role použita, hostitel ESX/ESXi nabídne přesun současných členů role do nové role nebo je jednoduše vyčlení z aktuální role. To snižuje pravděpodobnost, že omylem odstraníte použitou roli.

Když rozumíte tomu, jak pracovat s lokálními uživateli, skupinami, rolemi a povoleními na hostiteli ESX/ESXi, byste měli vědět, že většinu této práce pravděpodobně dělat nebudete. Správa lokálních uživatelských účtů je náročnější z důvodu nedostatku centralizované správy a ověřování

přístupu. Je tomu kvůli tomu, že většina strategií řízení přístupu by měla být soustředěna okolo uživatelských účtů, které přistupují k prostředí vCenter Server. Díky tomu můžete mít centralizovanou správu povolení a úložiště, integraci s infrastrukturou oprávnění adresářové služby Active Directory a podporu pro ověřování klientem vSphere Client.

Správa a údržba povolení systému vCenter Server

Model zabezpečení systému vCenter Server je téměř shodný s modelem zabezpečení hostitele ESX/ESXi z předchozí části kapitoly – vezmete uživatele nebo skupinu a přiřadíte je k roli k určitému objektu inventáře. Model zabezpečení systému vCener Server se liší v původu objektů uživatelů a skupin. V prostředí vCenter Server jsou uživatelé a skupiny ve skutečnosti uživateli a skupinami systému Windows, ale kterými, to záleží na tom, zda je počítač se systémem vCenter Server součástí domény. Jestliže počítač se systémem vCenter Server patří do pracovní skupiny, pak jsou uživatelé a skupiny uloženy v databázi SAM (Security Accounts Manager) na serveru a lze je spravovat pomocí uzlu **Local Users And Groups** modulu snap-in Computer Management. Pokud počítač se systémem vCenter Sever patří do domény adresářové služby Active Directory, pak je možné uživatele a skupiny přiřazovat k rolím z databáze Active Directory a můžete je spravovat pomocí modulu snap-in Active Directory Users And Groups. Toto je typické pro aplikace pro systém Windows a také vám to umožní spravovat všechny uživatele na síti na jediném místě – v adresářové službě Active Directory. Pokud nemůžete vytvářet uživatele a skupiny v adresářové službě Active Directory, budete muset poprosit příslušné správce, aby vám s tím pomohli. Jakmile vytvoříte uživatele a skupiny, můžete je přiřazovat k rolím v systému vCenter Server.

U dalšího popisu budu předpokládat, že máte systém vCenter Server umístěn na počítači, který je členem domény adresářové služby Active Directory, přestože procedura přiřazení povolení je stejná, i když máte počítač v pracovní skupině. Důležité je pamatovat si, kde vytvořit uživatele a skupiny, které budete potřebovat.

VCENTER SERVER V PRACOVNÍ SKUPINĚ VERSUS VCENTER SERVER V DOMÉNĚ

Systém vCenter Server můžete nainstalovat na počítač, který je součástí pracovní skupiny nebo domény. Ve většině případů nainstalujete systém vCenter Sevrer na počítač, který je součástí domény adresářové služby Active Directory. V důsledku toho se budete k systému vCenter Server přihlašovat pod doménovým uživatelským účtem. Tato centralizovaná správa účtů představuje bezpečnostní riziko, protože rozšiřujete oprávnění virtuální infrastruktury na uživatele, kteří původně tato oprávnění mít neměli. Podívejte se, jak:

Výchozí povolení systému vCenter Server udělí lokální skupině Administrators na počítači se systémem vCenter Server členství v roli Administrator v kořenu inventáře. Protože skupina Domain Admins je členem lokální skupiny Adminstrators, celá skupina Domain Admins má kompletní práva infrastruktury vCenter Server. Ve většině případů tato konfigurace poruší princip minimálních práv.

Abyste snížili riziko obsažené ve výchozí konfiguraci, vytvořte novou vyhrazenou skupinu v Active Directory, která bude obsahovat jen správce virtuální infrastruktury. Tato skupina pak může v seznamu povolení systému vCenter Server nahradit lokální skupinu Administrators. Až vytvoříte novou skupinu a udělíte ji práva, můžete odstranit položku povolení lokální skupiny Administrators z kořene inventáře systému vCenter Server, tím odstraníte toto bezpečnostní riziko.

Systém vCenter Server má více strukturovanou hierarchii s větší hloubkou než hostitel ESX/ESXi. Jak bylo řečeno dříve, jedinou možností, jak uspořádat virtuální stroje na jednotlivých hostitelích ESX/ESXi, je vytvořit společnou oblast prostředků a přesunout do ní příslušné virtuální stroje. Hierarchie systému vCenter Server přináší nové možnosti, jak vytvářet struktury složek pro organizaci objektů, jako jsou datová centra nebo virtuální stroje. Nejdříve samozřejmě musíte prohloubit své znalosti hierarchie systému vCenter Server.

Hierarchie systému vCenter Server

Jako server pro centrální správu všech hostitelů ESX/ESXi, virtuálních strojů, šablon, datových úložišť a sítí má systém vCenter Server bohatou hierarchii objektů. Abyste mohli plně využít výhod této hierarchie, musíte ji nejprve pochopit. Některé tyto informace jste mohli najít už v kapitole 3, ale nyní je chci trošku upřesnit. Začnu vysvětlením objektu datového centra.

Práce s objekty datového centra

V systému vCenter Server začnete vytvořením datového centra (označovaného také jako *objekt datového centra*). Objekt datového centra je základním stavebním kamenem hierarchie vCenter Server, stejně jako jsou organizační jednotky základními stavebními kameny struktury Active Directory. Než budete moci přidat prvního hostitele ESX/ESXi, musíte mít v systému vCenter Server vytvořený objekt datového centra. Nejste omezeni na jediný objekt datového centra, ve skutečnosti můžete mít dokonce několik objektů datového centra.

Následujícím postupem vytvoříte objekt datového centra:

1. Spusťte klienta vSphere Client a připojte se k instanci systému vCenter Server.
2. Zobrazte pohled **Hosts And Clusters**.
3. Klepněte pravým tlačítkem myši na objekt v inventáři a vyberte položku **New Datacenter**.
4. Zadejte název pro nový objekt datového centra.

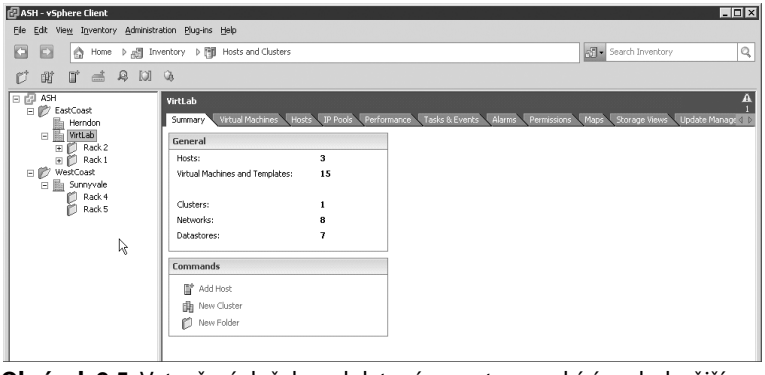
K čemu se tedy přesně objekt datového centra používá? Kromě toho, že ukládá hostitele ESX/ESXi, klastry, složky, virtuální stroje, společné oblasti prostředků, sítě a datová úložiště, slouží datové centrum také jako hranice. Datové centrum je hranice pro konfiguraci funkcí VMotion, VMware High Avaiability (HA) a VMware Distributed Resource Schedule (DRS). Jinými slovy – můžete například přenášet virtuální stroj funkcí VMotion jen na jiného hostitele ve stejném datovém centru. Funkce VMotion a VMware DRS najdete v kapitole 10, funkci VMware HA podrobněji popisuje kapitola 11, „Zajištění vysoké dostupnosti a nepřetržitého provozu".

Ačkoliv je objekt datového centra důležitý a každá hierarchie systému vCenter Server musí mít alespoň jeden objekt datového centra, jsou i jiné objekty, které budete při stavbě hierarchie systému vCenter Server používat. Dalším popsaným objektem bude složka.

Práce se složkami

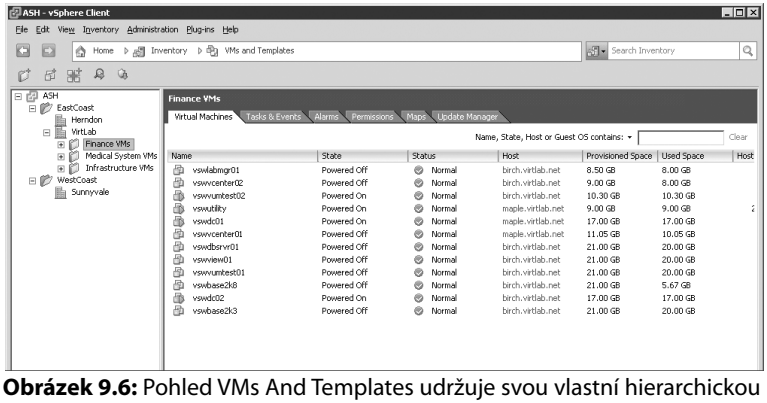
Co stane, když bude vaše společnost používat 30 datových center, některá umístěná v Evropě, jiná v Severní Americe a další v Jižní Americe a všechna budou mít jiné týmy správců? Jednoduchým řešením je vytvořit složky pod kořenovým objektem systému vCenter Server a potom do těchto složek vytvořit (nebo přesunout) objekty datových center. Vytvoření složek pod kořenem a umístění datových center do nich umožňuje širší správu řízení přístupu. Přemýšlejte, proč vytváříte složky na síťových discích – abyste uspořádali soubory a další složky a zjednodušili přiřazování povolení ke spoustě objektů. Navrhování inventáře systému vCenter Server vyžaduje stejnou logiku.

Stejným způsobem, jako používáte složky k uspořádání datových center, můžete rovněž vytvořit složky uvnitř datových center, abyste uspořádali virtuální stroje podle potřeby. Samozřejmě můžete jít ještě dále a vytvářet složky uvnitř složek. Obrázek 9.5 ukazuje strukturu, kde jsou datová centra uspořádána podle geografické polohy a servery jsou spravované podle rozvaděče, ve kterém jsou umístěné.



Obrázek 9.5: Vytvoření složek pod datovým centrem nabízí podrobnější řízení přístupu a strategie správy

Až dosud jste se setkali s používáním složek jen na uspořádání datových center a objektů v nich. Vzpomeňte si, že systém vCenter Server poskytuje dva hlavní pohledy na objekty inventáře – pohled **Hosts And Clusters** a **VMs And Templates**. Z velké části jste se setkali s použitím složek ve výchozím pohledu **Hosts And Clusters**, ale pohled **VMs And Templates** je neuvěřitelně užitečný při organizování virtuálních strojů s ohledem na potřeby správy a řízení přístupu běžných správců operačního systému Windows. Kromě toho si každý pohled inventáře, **Hosts And Clusters** a **VMs And Templates**, uchovává svou nezávislou hierarchii složek. Například změny objektů v pohledu **Hosts And Clusters** nemusí nutně ovlivnit objekty v pohledu **VMs And Templates**. Obrázek 9.6 ukazuje pohled **VMs And Templates** zkonstruovaný tak, aby podpořil implementaci řízení přístupu založenou typech virtuálních strojů v infrastruktuře. Pohled inventáře se skládá z několika vlastních složek s názvy Finance VMs, Medical System VMs a Infrastructure VMs. Tyto složky představují hranici pro přidělování oprávnění, stejně jako složky v pohledu **Hosts And Clusters**.



Obrázek 9.6: Pohled VMs And Templates udržuje svou vlastní hierarchickou strukturu, a tím vylepšuje možnosti řízení přístupu

Uchováním nezávislých hierarchií pomocí složek v každém z těchto pohledů získávají správci velké množství flexibility. Například byste mohli pohled **VMs And Templates** uspořádat podle jednotlivých oddělení společnosti, zatímco pohled **Hosts And Clusters** podle geografické pozice.V obou pohledech používají správci složky k tvorbě struktury, která nejlépe vyhoví potřebám společnosti.

Složky nejsou jediným nástrojem k tvorbě hierarchie, ale spolehlivě fungují jak u pohledu **Hosts And Clusters**, tak u pohledu **VMs And Templates**. Další nástroj k tvorbě hierarchie – společná oblast prostředků funguje pouze u pohledu **Hosts And Clusters**.

Uspořádání pomocí společných oblastí prostředků

Jak bylo řečeno dříve, společné oblasti prostředků lze použít k uspořádání virtuálních strojů. Hlavním rozdílem mezi „běžnou" složkou a společnou oblastí prostředků je, že společná oblast prostředků umožňuje správcům ovládat alokaci prostředků procesoru a paměti u virtuálních strojů v dané společné oblasti prostředků. Složky nenabízí tuto funkci. Společné oblasti prostředků můžete používat jen v pohledu **Hosts And Clusters** systému vCenter Server, složky můžete použít v pohledu **Hosts And Clusters** i v pohledu **VMs And Templates**. Společné oblasti prostředků zde nebudu dále rozebírat, protože už víte, jak je používat k uspořádání virtuálních strojů a přidělování povolení z části „Přidělování povolení pomocí společné oblasti prostředků".

Alokací prostředků společných oblastí prostředků se bude podrobněji zabývat kapitola 10.

Nyní už znáte různé části, ze kterých se skládá hierarchie systému vCenter Server – datová centra, složky, společné oblasti prostředků, hostitelé ESX/ESXi a klastry. Nyní bych rád dal vše dohromady, abyste viděli, jak kombinovat tyto objekty a vytvořit hierarchii, kterou vaše společnost potřebuje.

Složení hierarchie systému vCenter Server

Už jsem se zmínil, že systém vCenter Server je navržen jako podniková aplikace pro správu všech vašich hostitelů ESX/ESXi. Aby byl efektivní aplikací pro správu, systém vCenter Server potřebuje hierarchii, která bude odpovídat tomu, jak vaše společnost spravuje prostředky. Takže zůstává otázka – jak spravujete prostředky? Zakládá se strategie správy na geografii, odděleních nebo projektech? Nebo preferujete subjektivní přístup ke správě? Ať už používáte jakýkoliv přístup, systém vCenter Server podporuje tento přístup kombinování stavebních bloků, které již znáte – datová centra, složky a společné oblasti prostředků. Možná pomůže srovnání.

Představte si, co by se stalo, kdybyste všechny dokumenty ve vašem počítači uložili do kořenové složky pevného disku. Vyhledání dokumentů by bylo přinejmenším složité a přiřazování povolení k těmto objektů stejně tak. Stejně by to vypadalo, kdybyste všechny objekty virtuální infrastruktury umístili pod kořen.

Představte si například společnost s kancelářemi v Praze, Brně, Olomouci a Ostravě, kde každá kancelář má několik hostitelů ESX/ESXi, virtuálních strojů a šablon. Infrastruktura je vybudována tak, že hostitelé v Olomouci jsou připojeni ke sdílenému úložišti v Olomouci a hostitelé ESX/ESXi v Praze jsou připojeni k místnímu sdílenému úložišti své sítě. Tyto servery spolu mohou komunikovat přes síť WAN, ale můžou přistupovat pouze k úložišti ve své oblasti. Společnost má v každé kanceláři IT zaměstnance. Jak byste uspořádali hierarchii systému vCenter Server, aby nejlépe odpovídala této společnosti?

Nejjednodušší hierarchie systému vCenter Server by měla dvě datová centra – jedno pro Prahu a druhé pro Olomouc. V každém objektu datového centra by mohli místní zaměstnanci použí-

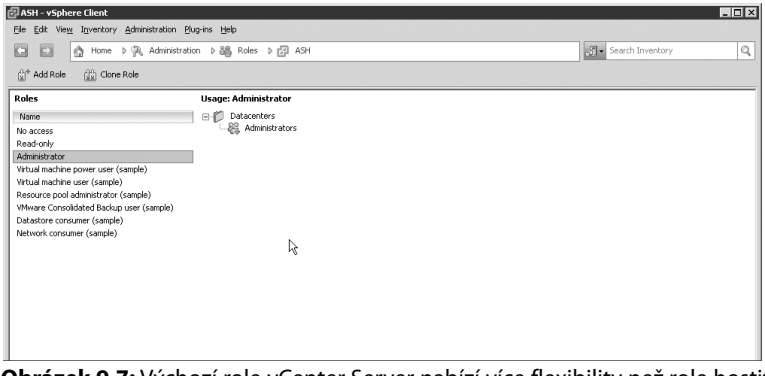
vat složky a společné oblasti prostředků k uspořádání virtuálních strojů, šablon a hostitelů ESX/ESXi.

Rovněž byste mohli vytvořit hierarchii podle oddělení, kde by ekonomické oddělení, marketingové oddělení a oddělní prodeje měla samostatné hostitele ESX/ESXi. V tomto případě by objekty datových center byly označené odděleními, a ne fyzickým umístěním.

V každém případě byste měli mít dobrou představu, jak pomocí různých stavebních bloků hierarchie vCenter Server vytvořit vhodný model pro svou společnost. Prozkoumejme role systému vCenter Server.

Role systému vCenter Server

Zatímco hostitel ESX/ESXi je trochu omezený svými výchozími rolemi, systém vCenter Server nabízí více výchozích rolí, tudíž poskytuje větší stupeň flexibility, co se řízení přístupu týče. Ačkoliv oba modely zabezpečení nabízí flexibilitu tvorbou vlastních rolí, hostitel ESX/ESXi obsahuje tři výchozí role, zatímco systém vCenter Server nabízí devět výchozích rolí, včetně těch stejných, co nabízí hostitel ESX/ESXi. Obrázek 9.7 zobrazuje výchozí role systému vCenter Server. Tyto role můžete vidět v klientu vSphere Client výběrem položky **View → Adminstration → Roles**.



Obrázek 9.7: Výchozí role vCenter Server nabízí více flexibility než role hostitele ESX/ESXi

Jak vidíte, systém vCenter Server poskytuje velké množství výchozích rolí. Vzpomeňte si, že není vhodné výchozí role hostitele ESX/ESXi měnit, u systému vCenter Server platí to stejné. Jestliže měníte výchozí role a ostatní správci o tom neví, můžou přiřazením výchozích rolí omylem přiřadit více nebo méně práv, než původně chtěli. Jestliže chcete vytvořit roli podobnou výchozí roli, zkopírujte tuto roli a změňte přiřazení práv. Ve skutečnosti vám systém vCenter server neumožní měnit role No Access, Read-Only Administrators, musíte je zkopírovat, abyste je mohli upravit.

Pokud chcete používat role efektivně, musíte pochopit funkce těchto rolí:

No Access: tato role nepovoluje uživateli nebo skupině žádný přístup. Ale k čemu je dobrá? Cílem je odebrat uživateli nebo skupině s povoleními na vyšší úrovni povolení k objektu na nižší úrovni, kterému je tato role přiřazena. Například jste Karlovi přidělili roli Virtual Machine User na úrovni objektu datového centra, ale existuje požadavek zabezpečení, který říká, že by Karel neměl mít přístup k jednomu účetnímu virtuálnímu stroji v datovém centru. Mohli byste Karlovi přidělit roli No Access na daném účetním virtuálním stroji, to by přebilo jeho práva role Virtual Machine User.

Read-Only: role Read-Only umožňuje uživatelům prohlížet inventář systému vCenter Server. Nijak jim nedovoluje pracovat s virtuálními stroji v klientu vSphere Client nebo s webovým klientem, až na to, že můžou sledovat, jestli jsou virtuální stroje vypnuté nebo zapnuté.

Administrator: uživatel přiřazený k objektu s rolí Administrator bude mít úplný přístup k tomuto objektu v systému vCenter Server. Všimněte si, že tím neudělíte žádná práva v hostujících operačních systémech ve virtuálních strojích. Například uživatel přiřazený roli Administrator pro virtuální stroj by měl mít možnost měnit paměť RAM a měnit jeho nastavení (sdílení, rezervace a omezení), ale neměl by povolení k přihlášení k virtuálnímu stroji, dokud mu jej někdo nepřidělí v hostujícím operačním systému.

Roli Administrator je možné přidělit objektu na libovolné úrovni hierarchie a uživatel nebo skupina přiřazená k této roli na dané úrovni bude mít v systému vCenter Server práva správce nad tímto objektem a všemi dceřinými objekty.

Kromě rolí No Access, Read-Only a Administrator jsou k dispozici ukázkové role. Ty mají za úkol předvést uživatelům, jak uspořádat role a povolení.

Virtual Machine Power User: ukázková role Virtual Machine Power User umožňuje uživatelům provádět většinu funkcí na virtuálních strojích. Mezi ně patří i konfigurace vyměnitelných médií, vypínání a zapínání, pořizování a mazání snímků obrazovky a úprava konfigurace. Tato povolení se týkají jen virtuálních strojů. Jestliže je tato role udělena uživatelům na úrovni datového centra, budou moci spravovat virtuální stroje datového centra, ale nebudou moci měnit nastavení jiných objektů tohoto datového centra, například společných oblastí prostředků.

Virtual Machine User: ukázková role Virtual Machine User umožňuje uživatelům pracovat s virtuálním strojem, ale nemůžou měnit jeho nastavení. Uživatelé můžou vypínat a zapínat virtuální stroj, měnit média virtuálních CD mechanik a disketových mechanik, pokud mají přístup k médiu, které chtějí měnit. Například uživatel s touto rolí bude moci měnit disk CD z obrazu ISO na sdíleném úložišti na fyzický disk CD ve svém vlastním klientském systému. Jestliže chcete, aby uživatel mohl měnit jeden ISO soubor za jiný (oba uložené na jednotce VMFS, Virtual Machine File System, nebo jednotce NFS, Network File System), musel by mít udělené povolení na rodičovském objektu datového úložiště v hierarchii systému vCenter Server – obvykle na datovém centru, na kterém je umístěn daný hostitel ESX/ESXi.

Resource Pool Administrator: ukázková role Ressource Pool Administrator uděluje uživateli povolení spravovat a nastavovat prostředky ve společné oblasti prostředků, včetně virtuálních strojů, dceřiných oblastí, naplánovaných úloh a výstrah.

VMware Consolidated Backup User: jak název role napovídá, ukázková role VMware Consolidated Backup uděluje uživateli práva pro tvorbu záloh virtuálního stroje pomocí VCB.

Datastore Consumer: ukázková role Datastore Consumer je určena uživatelům, kteří potřebují jediné povolení – povolení alokovat prostor datového úložiště. Tato role je velmi omezující.

Network Consumer: ukázková role Network Consumer má podobně jako role Datastore Consumer jediné právo, a to přiřazovat sítě.

Tyto výchozí role jsou dobrými výchozími body, ale nesplní všechny potřeby společnosti. Pokud potřebujete něco, co výchozí role nenabízí, musíte vytvořit vlastní roli. Tento proces vysvětlím v další části kapitoly.

Práce s rolemi systému vCenter Server

Co když role systému vCenter Server neposkytují nezbytné funkce pro určitou skupinu uživatelů? Řešení záleží na konkrétním problému. Podívejme se na základní problém. Vybrali jste vhodnou roli, ale schází jí klíčové povolení nebo nabízí několik povolení, která nechcete. Abyste splnili všechny požadavky, můžete jednoduše zkopírovat roli a potom ji upravit.

Následujícím postupem zkopírujete roli v systému vCenter Server:

1. Spusťte klienta vSphere Klient a připojte se k instanci systému vCenter Server.
2. Přepněte na pohled **Roles** pomocí nabídky, navigačního panelu nebo klávesové zkratky.
3. Klepněte pravým tlačítkem myši na roli, kterou chcete zkopírovat, a z kontextové nabídky vyberte položku **Clone**.

Jakmile zkopírujete roli, můžete do ní přidávat nebo z ní odstraňovat práva, jak budete potřebovat. Proces editace role jsem popsal dříve v této kapitole, v části „Úprava a odstranění rolí".

Práva systému vCenter Server

Role jsou užitečné, když jste pomalu začali pronikat do vlastností rolí a zjistili, jak je editovat, musíte pochopit jednotlivá práva a co vám můžou přinést při úpravě rolí. Vzpomeňte si, že práva jsou jednotlivé úlohy, které přiřazujete rolím. Bez přiřazených práv jsou role k ničemu, proto je důležité, abyste pochopili dostupná práva systému vCenter Server.

Jde o poměrně dlouhý seznam práv, který je však rozdělen do kategorií, takže můžete začít tím, že se naučíte, co jednotlivé kategorie dovolují:

Alarms: řídí schopnost vytvářet, upravovat, mazat, zakazovat a oznamovat výstrahy systému vCenter Server.

Datacenter: řídí schopnost vytvářet, mazat, přesouvat a přejmenovávat datová centra v systému vCenter Server.

Datastore: řídí, kdo smí přistupovat k souborům uloženým na jednotce hostitele ESX/ESXi. Toto povolení musíte přiřadit rodičovskému objektu samotného hostitele ESX/ESXi – například datovému centru, kastru ESX/ESXi nebo složce obsahující hostitele ESX/ESXi.

Distributed Virtual Port Group: řídí, kdo smí vytvářet, mazat, odstraňovat a upravovat distribuované skupiny virtuálních portů na distribuovaných virtuálních přepínačích.

Distributed Virtual Switch: řídí vytváření, mazání, úpravu a přesouvání přepínačů vNetwork Distributed Switches, přidávání a odstraňování hostitelů ESX/ESXi a konfiguraci portů na distribuovaném virtuálním přepínači.

Extension: řídí schopnost registrovat, aktualizovat a odregistrovat rozšíření v systému vCenter Server. Mezi dvě dostupná rozšíření patří VMware Update Manager a VMware Converter.

Folder: řídí vytváření, odstraňování a úpravu složek v hierarchii systému vCenter Server.

Global: zahrnuje schopnost spravovat nastavení licence systému vCenter Server a nastavení serveru, například nastavení protokolu SNMP a SMTP.

Host: řídí, co smí uživatelé dělat s hostitelem ESX/ESXi v inventáři. Sem patří i úlohy jako přidávání a odstraňování hostitelů ESX/ESXi z inventáře, změna nastavení paměti hostitele nebo změna nastavení brány firewall.

Host Profile: řídí vytváření, editaci, mazání a prohlížení profilů hostitelů.

Network: řídí nastavení a odstranění sítí z inventáře systému vCenter Server.

Performance: řídí schopnost upravovat intervaly, kdy se zobrazují data v grafech na záložce Performance objektu.

Permissions: řídí, kdo smí upravovat práva přiřazená roli a kdo smí upravovat kombinaci role a uživatele na určitém objektu.

Resource: řídí úpravu společných oblastí prostředků, včetně vytváření, mazání a přejmenování oblastí, také řídí migrace VMotion a uplatnění doporučení DRS.

Scheduled Task: řídí konfiguraci a spouštění naplánovaných úloh systému vCenter Server.

Sessions: řídí schopnost prohlížet a odpojovat relace klientů vSphere Client připojených k systému vCenter Server a odesílat zprávy připojeným uživatelům. Jak ukazuje obrázek 9.8, uživatel bez práv Sessions nemůže ukončovat relace klientů vSphere Client.

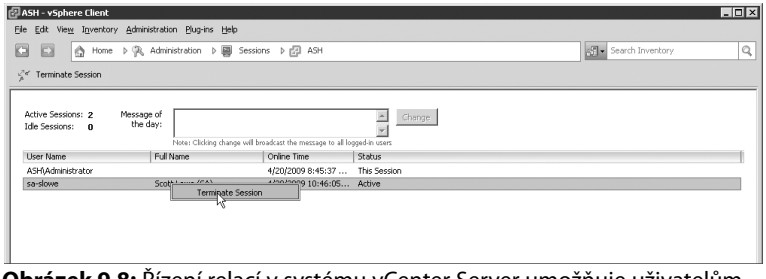
Storage Views: řídí změnu nastavení serveru a prohlížení pohledů úložiště.

Tasks: řídí schopnost vytvářet a aktualizovat úlohy.

vApp: řídí konfiguraci a správu aplikací vApp, například schopnost přidávat virtuální stroje k aplikaci vApp, kopírovat, vytvářet, mazat, exportovat, importovat, vypínat a zapínat aplikaci vApp a prohlížet prostředí OVF (Open Virtualization Format).

Virtual Machine: řídí práci s virtuálními stroji v inventáři vCenter Server, včetně schopnosti vytvářet, mazat a připojovat se ke vzdálené konzole virtuálního stroje; vypínat a zapínat virtuální stroj; měnit vyměnitelná média; pracovat se šablonami atd.

VMware vCenter Update Manager: řídí, kdo smí aktualizovat systém a nastavovat službu vCenter Update Manager.



Obrázek 9.8: Řízení relací v systému vCenter Server umožňuje uživatelům odpojovat relace klientů vSphere Client

Záleží na tom, jak tato různá práva přiřadíte k rolím. Jak jste viděli dříve, systém vCenter Server má několik výchozích rolí. Některé z nich jsou pevné a nelze je měnit – No Access, Read-Only a Administrator. Ostatní předem definované role najdete v tabulce 9.1 spolu s právy, která jsou těmto rolím standardně přiřazena.

Jak vidíte, systém vCenter Server je poměrně specifický, co se týče práv, která můžete přiřazovat rolím. Protože jsou tato práva specifická, může to někdy zkomplikovat proces udělování povolení uživatelům k vykonání zdánlivě jednoduchých úloh. Zopakujme si několik příkladů, abyste lépe pochopili, jak kombinovat práva, role povolení v systému vCenter Server.

> **UDĚLOVÁNÍ PRÁVA VYTVÁŘET VIRTUÁLNÍ STROJE A INSTALOVAT HOSTUJÍCÍ OPERAČNÍ SYSTÉM**
>
> Jednou z obvyklých úloh virtuální infrastruktury je udělit uživatelům nebo skupinám práva vytvářet virtuální stroje. Když prohlédnete seznam dostupných práv, bude se vám tato úloha zdát pravděpodobně jednoduchá. Je však o něco složitější, než se na první pohled zdá. Aby uživatel mohl vytvářet virtuální stroje, musíte mu přiřadit několik práv na různých úrovních inventáře systému vCenter Server.

Kombinování práv, rolí a povolení v systému vCenter Server

Dosud jsem vám ukázal různé kousky, které musíte znát, abyste mohli uspořádat systém vCenter Server, aby podporoval požadavky na správu a operační požadavky vaší společnosti. Jak tyto kousky dát dohromady, může být někdy složitější, než se na první pohled může zdát. Následujících několik odstavců popíše, jak tyto kousky spojit.

Zde je příklad. Ve vašem IT oddělení máte skupinu, která se stará o tvorbu všech serverů se systémem Windows. Jakmile jsou servery vytvořeny, řízení se předá dál vyhrazené skupině. Když virtualizujete datové centrum, musíte stejným způsobem oddělit úlohy v systému vCenter Server. Zní to jednoduše, že? Musíte nastavit systém vCenter Server, aby tato skupina mohla vytvářet virtuální stroje. Tato skupina je reprezentována v adresářové službě Active Directory jako objekt skupiny (tato skupina je pojmenovaná IT-Provisioning) a pravděpodobně byste rádi využili členství v této skupině, abyste mohli řídit, kdo smí udělovat tato povolení v systému vCenter Server.

V následujícím postupu stručně popíšu některé kroky. Například nebudete rozebírat, jak vytvářet role a jak je přiřazovat objektům inventáře jako povolení, protože to popisovala jiná část této kapitoly.

Následujícím postupem umožníte skupině systému Windows vytvářet virtuální stroje:

1. Připojte se klientem vSphere Client k instanci systému vCenter Server. Přihlaste se s uživatelským účtem, kterému jste v systému vCenter Server přiřadili roli Administrator.
2. Vytvořte novou roli s názvem VMCreators.
3. Roli VMCreators přiřaďte následující práva:
   - Virtual Machine → Inventory → Create
   - Virtual Machine → Configuration → Add New Disk
   - Virtual Machine → Configuration → Add Existing Disk
   - Virtual Machine → Configuration → Raw Device
4. Vytvořte novou roli s názvem VMAssigners.
5. Přiřaďte následující práva roli VMAssigners:
   - Resource → Assign Virtual Machine To Resource Pool

Tabulka 9.1: Tabulka práv výchozích rolí

Předem definovaná role	Přiřazená práva
Virtual Machine Power User	Datastore → Browse Datastore Global → Cancel Task Scheduled Task → Create Task, Delete Task, Remove Task, Run Task Virtual Machine → Configuration → Add Existing Disk, Add New Disk, Add or Remove Device, Advanced, Change CPU Count, Change Resource, Disk Lease, Memory, Modify Device Settings, Remove Disk, Rename, Reset Guest Information, Settings, Upgrade Virtual Hardware Virtual Machine → Interaction → Answer Question, Configure CD Media, Configure Floppy Media, Konsole Interaction, Device Connection, Power On, Power Off, Reset, Suspens, VMware Tools Install Virtual Machine → State → Create Snapshot, Remove Snapshot, Rename Snapshot, Revert To Snapshot
Virtual machine User	Global → Cancel Task Sheduled Task → Create Task, Delete Task, Remove Task, Run Task Virtual Machine → Interaction → Answer Question, Configure CD Media, Configure Floppy Media, Console Interaction, Device Connection, Power On, Power Off, Reset, Suspend, VMware Tools Install
Resource pool Administrator	Alarms → Create Alarm, Modify Alarm, Remove Alarm Datastore → Browse Datastore Folder → Create Folder, Delete Folder Move Folder, Rename Folder Global → Cancel Task, Log Ebeny, Set Cystom Attribute Permissions → Modify Permissions Resource → Assign Virtual Machine To Resource Pool, Create Resource Pool, Migrate, Modify Resource Pool, Move Resource Pool, Query VMotion, Relocate, Remove Resource Pool, Rename Resource Pool Scheduled Task → Create Task, Delete Task, Remove Task, Run Task Virtual Machine → Configuration → Add Existing Disk, Add New Disk, Add Or Remove Device, Advanced, Change CPU Count, Change Resource, Disk Lease, Memory, Modify Device Settings, Raw Device, Remove Disk, Rename, Reset Guest Information, Settings, Upgrade Virtual Hardware Virtual Machine → Interaction → Answer Question, Configure CD Media, Configure Floppy Media, Console Interaction, Device Connection, Power On, Power Off, Reset, Suspens, VMware Tools Install Virtual Machine → Inventory → Create, Move, Remove Virtual Machine → Provisioning → Allow Disk Access, Allow Read-Only Disk Access, Allow Virtual Machine Download, All Virtual Machine Files Upload, Clone Template, Clone Virtual Machine, Create Template From Virtual Machine, Customize, Deploy Template, Mark As Template, Mark As Virtual Machine, Modify Customization Specification, Read Customization Specifications Virtual Machine → State → Create Snapshot, Remove Snapshot, Rename Snapshot, Revert To Snapshot

Předem definovaná role	Přiřazená práva
VMware Consolidated Backup User	Virtual Machine → Configuration → Disk Lease Virtual Machine → Provisioning → Allow Read-Only Disk Access, Allow Virtual Machine Donwload Virtual Machine → State → Create Snapshot, Remove Snapshot
Datastore Consumer	Datastore → Allocate Space
Network Consumer	Network → Assign Network

6. Přiřaďte skupině IT-Provisioning ze systému Windows roli VMCreators na složce nebo objektu datového centra.
7. Přiřaďte té stejné skupině roli VMAssigners na společné oblasti prostředků, hostiteli a klastru.
8. Stejné skupině přiřaďte roli Read-Only na objektu datového centra nebo složce obsahující objekt datového centra. Zakažte propagaci, pokud je tato role přiřazena přímo datovému centru. Ponechejte propagaci, jestliže je role přidělena složce obsahující objekt datového centra.

Nyní jsou práva pro tvorbu virtuálního stroje kompletní, ale skupina IT-Provisioning z kroků 6 až 8 nemá práva k zavedení obrazu disku CD/DVD, a tudíž nemůže instalovat hostující operační systém. Proto potřebuje tato skupina více práv, aby kromě vytváření virtuálních strojů a jejich umístění na správné místo v systému vCenter Server mohla také instalovat hostující operační systém na tyto virtuální stroje.

Následujícím postupem umožníte skupině IT-Provisioning instalovat hostující operační systém ze souboru s obrazem disku CD/DVD:

1. Připojte se klientem vCenter Client k instanci systému vCenter Server. Přihlaste se pod uživatelským účtem s přiřazenou rolí Administrator v systému vCenter Server.
2. Vytvořte novou roli s názvem GOS-Installers.
3. Roli GOS-Installers přiřaďte následující práva:
   - Datastore → Browse Datastore
   - Virtual Machine → Configuration
   - Virtual Machine → Interaction
4. Přiřaďte skupině IT-Provisioning roli GOS-Installers na objektu datového centra.

Jak můžete vidět, zdánlivě jednoduchá úloha vytvoření virtuální stroje potřebuje ve skutečnosti tři různé role a tři různé sady práv.

Když udělujete oprávnění, vždy jednejte opatrně. Nedávejte více povolení, než je nutné k provedení dané úlohy. Stejně jako v jiných počítačových systémech, je implementace řízení přístupu živým objektem, který potřebuje neustálé revize a aktualizace. Spravujte povolení opatrně, buďte flexibilní a očekávejte, že uživatelé a správci budou zvědaví a budou se snažit využít svou úroveň přístupu naplno. Buďte vpředu a nezapomínejte na princip minimálního oprávnění.

Jelikož už víte, jak přiřazovat povolení, role a práva v systému vCenter Server, zbývá ještě jedna oblast, která by vás měla zajímat. Co byste dělali, kdybyste neměli možnost použít klienta vSphere Client? Jaké funkce systém VMware vSphere nabízí, pokud nějaké? A jak se to vztahuje k řízení přístupu systému vCenter Server? Na všechny otázky odpoví následující část kapitoly.

DO DETAILU

PRÁCE S POVOLENÍMI SYSTÉMU VCENTER SERVER

Ve společnostech, ať už malých nebo velkých, patří obvykle uživatelé do několika skupin a těmto skupinám jsou přiřazeny různé stupně povolení na různých objektech. V tomto příkladu budu mluvit o vlivu členství ve více skupinách a více přiřazených povoleních ve virtuální infrastruktuře.

Podívejme se nejprve na efektivní povolení, když uživatel patří do více skupin, které mají různá povolení na objektech na různých úrovních inventáře. V tomto příkladu je uživatel se jménem Jan Novák členem skupin Res_Pool_Admins a VM_Auditors. Skupině Res_Pool_Admins je přiřazena role Resource Pool Admins a povolení je nastaveno na společné oblasti prostředků Production. Skupině VM_Auditors je přiřazena role Read-Only a povolení je nastaveno na virtuální stroj Win2008-02. Virtuální stroj Win2008-02 je umístěn ve společné oblasti prostředků Production.

Když se uživatel přihlásí k počítači se systémem vCenter Server jako Jan Novák, inventář zobrazí jen ty objekty, které mu povolení zpřístupní. Díky přiřazeným povolením bude moci uživatel Jan Novák spravovat společnou oblast prostředků Production a bude mít plná práva nad virtuálním strojem Win2008-01, ke kterému se přenáší i práva role Resource Pool Admin. Uživatel Jan Novák však nebude moci spravovat virtuální stroj Win2008-02, protože k němu má pouze práva role Read-Only. Z toho příkladu byste si měli vzít ponaučení, že uživatelům ve více skupinách s konfliktními právy na objektech na nižší úrovni inventáře jsou udělena jen ta práva, která se týkají přímo daného objektu.

Z dalšího příkladu byste měli pochopit, co to je efektivní povolení, když uživatel patří do více skupin s různými povoleními na stejných objektech. V tomto příkladě je uživatel Franta Vopršálek členem skupin VM_Admins a VM_Auditors. Skupině VM_Admins je přiřazena role Virtual Machine Power User a skupině VM_Auditors je přiřazena skupina Read-Only. Obě tyto role jsou přiřazeny jako povolení na společné oblasti prostředků Production.

Když se uživatel přihlásí k systému vCenter Server jako Franta Vopršálek, inventář bude obsahovat jen mu dostupné objekty. Podle popsaných povolení bude moci Franta Vopršálek upravovat všechny virtuální stroje ve společné oblasti prostředků Production. Je tomu tak proto, že práva role Virtual Machine Power User plynoucí z členství ve skupině VM_admin zvítězí nad právy role Read-Only plynoucími ze členství ve skupině VM_Auditors.

Z tohoto příkladu je vidět, že efektivní povolení je narůstající povolení, pokud uživatel patří do více skupin s různými povoleními na stejném objektu. Kdyby Franta Vopršálek patřil do skupiny s přiřazenou rolí No Access, jeho role Virtual Machine Power User by převládla. Kdyby však byla role No Access uživatele Franty Vopršálka přiřazena přímo objektu systému vCenter Server, pak by neměl přístup k žádnému objektu, ke kterému by se toto povolení přeneslo.

I když dobře chápete přenos povolení, vždy byste měli jednat opatrně a řídit se pravidlem minimálního oprávnění, kdy uživatel nemá více práv, než potřebuje k provedení dané úlohy.

Správa virtuálních strojů pomocí webové konzoly

Představte si situaci, že jste mimo kancelář a někdo vám zavolá, případně sami uvidíte, že je nějaký problém s virtuálním strojem ve vašich datových centrech. Takové situace se stávají. Kancelář je daleko a vy s sebou nemáte svůj notebook. Jak se můžete rychle podívat na virtuální

stroj a odhalit, kde je problém? Přestože na místě, kde právě jste, máte k dispozici počítač, tento počítač nemá nainstalovaného klienta vSphere Client, bez kterého nemůžete spravovat své prostředí VMware vSphere. Je možné tuto situaci nějak vyřešit?

Naštěstí společnost VMware nabízí webovou konzolu pro správu, kterou můžete instalovat na váš počítač se systémem vCenter Server a která se automaticky nainstaluje na všechny hostitele ESX/ESXi. Vše, co tato konzola potřebuje, je webový prohlížeč a připojení k Internetu. Díky tomu byste měli mít přístup k prostředí VMware vSphere, i když nemáte po ruce klienta vSphere Client.

POŽADAVKY NA PROHLÍŽEČ WEBOVÉ SPRÁVY SYSTÉMU VCENTER SERVER

Abyste se mohli připojit k systému vCenter Server pomocí webové konzoly, musíte mít některý z uvedených prohlížečů:

- Internet Explorer 6.0 nebo novější (pouze Windows),
- Netscape Navigator 7.0 nebo novější,
- Mozilla 1.x nebo novější,
- Firefox 1.0.7 nebo novější.

Tato webová konzola vám zpřístupní virtuální stroje ve vaší infrastruktuře a je založena na webové službě Apache Tomcat. Webová služba Apache Tomcat je součástí instalace systému vCenter Server, jak víte z kapitoly 3. Tomcat je obvykle známý z operačních systémů Linux, kde se používá jako webový server. Verze Tomcatu pro Windows slouží jako komponenta pro webový přístup k systému vCenter Server místo součásti Windows IIS (Internet Information Services). Tato komponenta, podobně jako klient vSphere Client, ctí úroveň zabezpečení definovanou povoleními systému vCenter Server.

Následujícím postupem můžete spravovat virtuální stroje na počítači se systémem vCenter Server pomocí webové konzoly:

1. Otevřete webový prohlížeč a zadejte IP adresu nebo úplný doménový název počítače se systémem vCenter Server.
2. Na úvodní webové stránce systému vCenter Server klepněte na odkaz **Log In To Web Access**.
3. Na přihlašovací stránce **vSphere Web Access** zadejte platné uživatelské jméno a heslo.

Jakmile zadáte platné uživatelské jméno a heslo uživatele, který má povolení v systému vCenter Server, uvidíte inventář s virtuálními stroji, jak ukazuje obrázek 9.9.

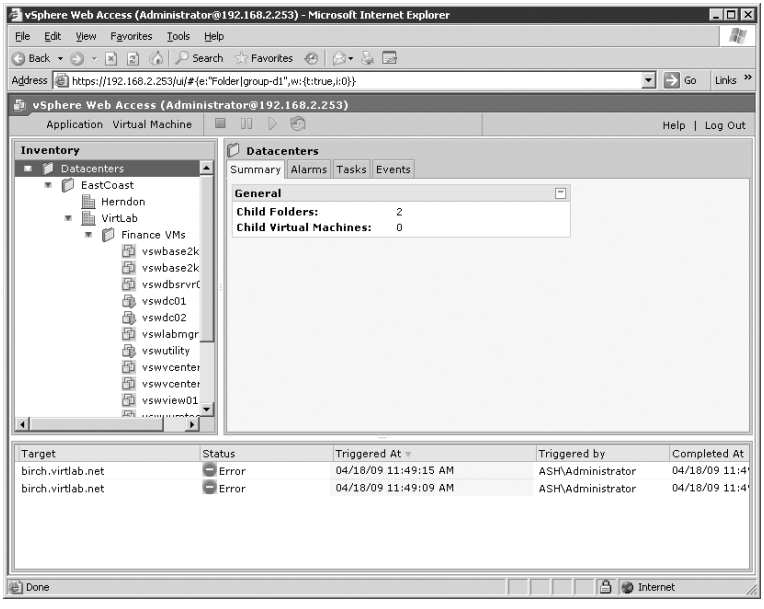
SPRÁVA VIRTUÁLNÍHO STROJE PŘES WEBOVÉ ROZHRANÍ

Webová konzola systémem vCenter Server slouží výhradně k přístupu a správě virtuálních strojů. V inventáři neuvidíte žádné hostitele ESX/ESXi, všechny úlohy související se správou hostitelů musíte provádět z klienta vSphere Client nebo z příkazového řádku.

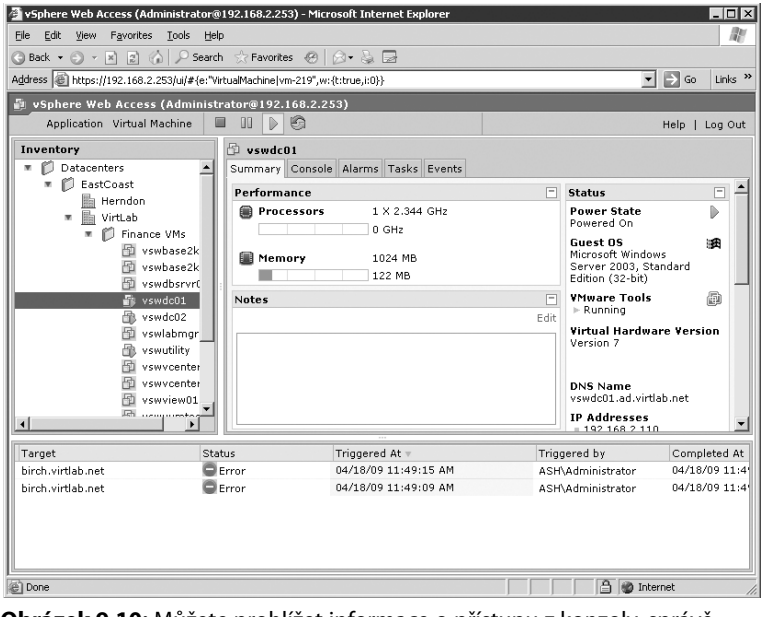
Po výběru virtuálního stroje se změní rozvržení webové konzoly, protože se objeví další záložky a odkazy pro správu virtuálního stroje. Obrázek 9.10 ukazuje výchozí pohled pro výběru virtuálního stroje z inventáře. Panel nástrojů navrchu stránky obsahuje kromě pěti záložek ještě tlačítka pro vypínání a zapínání virtuálního stroje.

Záložka **Events** obsahuje poslední události, které vznikly na vybraném virtuálním stroji. Události v tomto pohledu obsahují informace o vypnutí nebo zapnutí a o využití prostředků.

Záložka **Alarms** umožňuje prozkoumat výstrahy, které virtuální stroj spustil, protože je měl nastavené. Vytváření a správu výstrah popisuje podrobněji kapitola 12, „Správa výkonu systému vSphere Performace“.



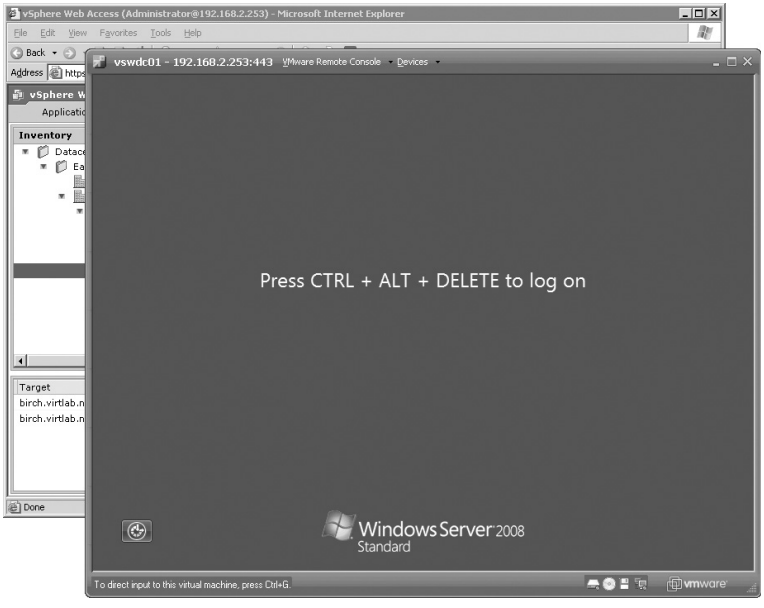
Obrázek 9.9: vCenter Server Web Access vám umožňuje přístup k dostupným virtuálním strojům a jejich správu



Obrázek 9.10: Můžete prohlížet informace o přístupu z konzoly, správě hardware a vypnutí nebo zapnutí

Záložka **Tasks** obsahuje úlohy, které nedávno proběhly na virtuálním stroji, a také úlohy, které stále probíhají.

Jak ukazuje obrázek 9.11, záložka **Console** poskytuje přístup k virtuálnímu stroji podobně jako klávesnice nebo myš přímo připojené k fyzickému serveru. Všimněte si, že když poprvé zobrazíte záložku **Console** ve webovém prohlížeči, budete vyzváni k instalaci doplňku, který zprostředkovává funkce konzoly pod záložkou **Console**.



Obrázek 9.11: Záložka Console otevře nové okno a umožní vám přístup k virtuálnímu stroji, pokud nemáte k dispozici tradiční nástroje

SPOJENÍ WEBOVÝCH SLUŽEB

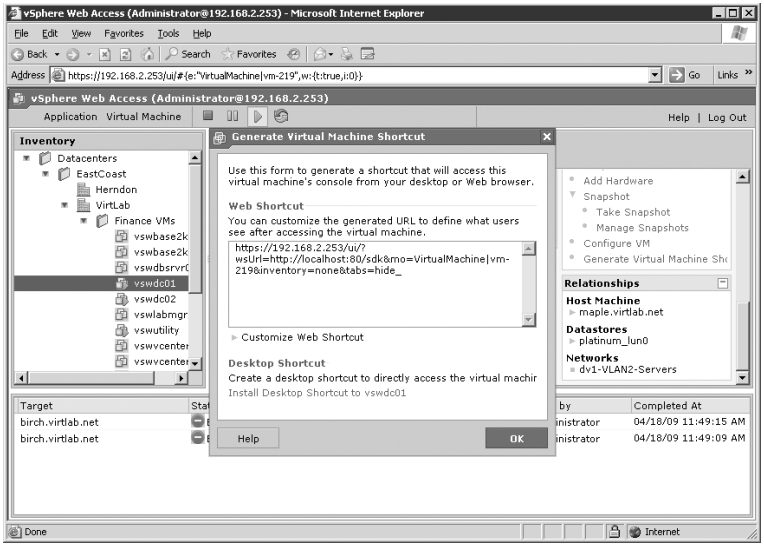
Webová konzola není náhrada za Terminal Services, Remote Desktop, VNC, Citrix nebo jakýkoliv jiný nástroj pro vzdálenou správu. Nejužitečnější je webová konzola v dříve popsaných situacích, kdy se nemůžete k serveru připojit běžnými nástroji. Webová konzola umožňuje vyřešit problém s virtuálním strojem téměř odkudkoliv. Webová konzola má však problém se současným připojením více uživatelů. Protože je toto spojení považováno za konzolové, více uživatelů sdílí myš a klávesnici, to je odlišné od spojení Remote Desktop nebo Terminal Services, kde uživatelé o sobě bez bližšího zkoumání vzájemně neví.

K virtuálnímu stroji se můžete pomocí webové konzoly přihlásit stisknutím klávesové zkratky **Ctrl+Alt+Insert** nebo klepnutím na nabídku Virtual Machine v panelu nástrojů a potom vybráním položky **Troubleshoot → Send Ctrl+Alt+Delete**.

Pokud vyberte virtuální stroj, část **Commands** na pravé straně stránky bude obsahovat odkaz Generate Virtual Machine Shortcurt, který generuje URL adresu pro přímý přístup ke konzole virtuálního stroje. Obrázek 9.12 obsahuje stránku pro generování URL adresy. Standardně jsou políčka Limit View To The Remote Console a Limit View To A Single Virtual Machine zaškrtnutá, to omezí URL adresu vzdálené konzoly na cílový virtuální stroj. URL adresa začíná IP adresou

nebo úplným doménovým jménem systému vCenter Server v závislosti na tom, jak bylo spojení zadáno ve webovém prohlížeči.

URL adresa je poměrně dlouhá, a proto se špatně pamatuje. Uživatelé, kteří potřebují přistupovat k virtuálnímu stroji občas, si můžou URL adresu vzdálené konzoly zkopírovat a vložit do e-mailu nebo poslat jako okamžitou zprávu (IM). Jakmile uživatel klepne na daný odkaz, otevře se ověřovací stránka. Identifikátor, se kterým se uživatel přihlašuje, musí mít přiřazenou přinejmenším roli Virtual Machine User, aby se přihlášení zdařilo.



Obrázek 9.12: Vygenerovaná URL adresa pro virtuální stroj poskytuje přímý přístup, ale musí proběhnout správné ověření přihlašovacích údajů a práv

URL ADRESY VZDÁLENÉ KONZOLY

Komponenta webového přístupu u hostitelů ESX/Esti je v podstatě stejná jako uvedená komponenta pro systém vCenter Server. Můžete však prohlížet jen virtuální stroje na určitém hostiteli. Jestliže vygenerujete URL adresu vzdálené konzoly připojením k hostiteli ESX/ESXi, URL adresa bude začínat IP adresou nebo úplným doménovým jménem hostitele, a ne počítače se systémem vCenter Server. Problém nastane, když přesunete virtuální stroj na nového hostitele pomocí VMotion nebo VMware HA. Přesun virtuálního stroje zruší platnost této URL adresy. Kvůli tomu byste vždy měli vytvářet URL adresy vzdálené konzoly připojením k vCenter Server, a ne k hostiteli ESX/ESXi.

Cvičení

Správa a údržba povolení hostitelů ESX/ESXi: Hostitelé VMware ESX a VMware ESXi poskytují strukturovaný přístup k povolením založeným na uživatelích, skupinách, rolích a právech. Tento přístup nabízí jemné řízení přístupu k virtuálním strojům a prostředkům.

> **Cvičení:** Udělili jste povolení jednomu správci na hostiteli ESX tak, že jste účet tohoto správce přidali k roli Administrator. Nyní se tento správce pokouší spravovat několik virtuálních strojů na jiném hostiteli, ale nemůže. Zjistili jste, že tento správce má účet na tomto hostiteli. Kde by mohl být problém?

Správa a údržba povolení systému vCenter Server: systém vCenter Server centralizuje správu uživatelů, skupin a povolení spojením s adresářovou službou Active Directory. Systém vCenter Server navíc rozšiřuje strukturovaný přístup založený na uživatelích, skupinách, rolích a právech nejen na hostitele ESX/ESXi, ale i na datová úložiště, sítě, společné oblasti prostředků, správce vCenter Update Manager, aplikace vApps, profily hostitelů atd.

> **Cvičení:** Skupina správců potřebuje úplný přístup k určité sadě virtuálních strojů. Všechny tyto virtuální stroje jsou umístěny ve společné oblasti prostředků. Tato společná oblast prostředků obsahuje i několik dalších virtuálních strojů, ke kterým by tito správci neměli mít přístup. Aniž byste museli tyto další virtuální stroje odsunout ze společné oblasti prostředků, jak byste nejlépe udělili povolení k této sadě virtuálních strojů?

Správa vituálního stroje pomocí webové konzoly: systém vCenter Server nenabízí jen klienta vSphere Client, ale i webový přístup k vykonání základních úloh správy, například vypnutí nebo zapnutí, správa snímků obrazovky nebo prohlížení virtuálního stroje.

> **Cvičení:** Je možné s konzolou vCenter Server Web Access vygenerovat URL adresu pro prohlížení jen určitého virtuálního stroje? Pokud ano, jak?