IBM Spectrum Protect for Virtual Environments
Verze 8.1.10

Instalační příručka k produktu Data Protection for VMware

Poznámka:

Dříve než použijete tyto informace a produkt, který podporují, přečtěte si informace, které uvádí část “Upozornění” na stránce 117.

Toto vydání se vztahuje na verzi 8, vydání 1, úpravu 10 produktu IBM Spectrum Protect for Virtual Environments (číslo produktu 5725-X00) a na všechna následná vydání a úpravy, dokud nebude v nových vydáních uvedeno jinak.

Obsah

O této publikaci

IBM Spectrum Protect for Virtual Environments poskytuje mimohostitelské přírůstkové zálohování na úrovni bloků a obnovení souborů a okamžitou obnovu z úplné zálohy virtuálního počítače pro počítače hosta v systému Windows nebo Linux. Přírůstková zálohování na úrovni bloku jsou dostupná při použití produktu IBM Spectrum Protect for Virtual Environments s modulem pro přesouvání dat IBM Spectrum Protect.

Komu je tato příručka určena ke čtení

Tato publikace je určena pro uživatele a administrátory, kteří chtějí nainstalovat a nakonfigurovat produkt IBM Spectrum Protect for Virtual Environments.

Informace o přehledu, úlohy uživatelů, scénáře záloh a obnov, popis příkazů a chybové zprávy jsou zdokumentovány v uživatelské příručce *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware*.

Příručky

Řada produktů IBM Spectrum Protect zahrnuje IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases a několik dalších produktů správy úložišť od společnosti IBM®.

Chcete-li zobrazit dokumentaci o produktu IBM, prohlédněte si téma Centrum znalostí IBM.

Novinky ve verzi 8.1.10

IBM Spectrum Protect for Virtual Environments verze 8.1.10 uvádí defekty a opravy APAR týkající se aktualizací.

Seznam nových funkcí a aktualizací v tomto vydání a v předchozích vydáních verze 8 naleznete na webu Aktualizace Data Protection for VMware.

Pokud byly v dokumentaci provedeny změny, jsou označeny svislou čárou (|) na okraji.

Kapitola 1. Instalace a upgrade produktu Data Protection for VMware

Instalace produktu IBM Spectrum Protect for Virtual Environments zahrnuje plánování, instalaci a počáteční konfiguraci.

Instalovatelné komponenty

Produkt Data Protection for VMware zahrnuje několik komponent, které můžete nainstalovat k ochraně svého virtuálního prostředí.

Dostupnost komponent závisí na prostředí operačního systému. Chcete-li určit, které komponenty jsou ve vašem prostředí k dispozici, přezkoumejte tabulku.

Na systémech Windows a Linux jsou všechna umístění pevnými umístěními. Umístění Windows jsou uvedena v níže uvedené tabulce. Linux: komponenta Spectrum Protect for VE je nainstalována v adresáři `/opt/tivoli/tsm/tdpvmware`. Klient a rozhraní API pro zálohování a archivaci Linux Spectrum Protect jsou nainstalováni instalačním programem VE do pevných umístění: `/opt/tivoli/tsm/client/api` a `/opt/tivoli/tsm/client/ba`.

Každý instalační balík vám zobrazení licenční smlouvu s koncovým uživatelem. Pokud nepřijmete licenční smlouvu, instalační proces se zastaví.

Tabulka 1. Dostupné komponenty produktu Data Protection for VMware podle operačního systému

Komponenta	Linux®	Windows
Agent zotavení produktu IBM Spectrum Protect Tato komponenta poskytuje funkce virtuálního připojení a okamžité obnovy. Pevné umístění instalace na systému Windows: `C:\Program Files\Tivoli\TSM\RecoveryAgent`		√
Rozhraní příkazového řádku agenta zotavení Rozhraní příkazového řádku se používá pro operace připojení. Pevné umístění instalace na systému Windows: `C:\Program Files\IBM\SpectrumProtect\Framework`		√
Dokumenty Dokumenty zahrnují soubory Readme a soubory s upozorněními.	√	√
Soubor zpřístupnění produktu Data Protection for VMware Tato komponenta umožňuje produktu IBM Spectrum Protect Data Protection for VMware spouštět následující typy záloh: • trvale přírůstková záloha • trvale přírůstková úplná záloha Tato komponenta je požadována pro ochranu aplikace. Pokud odlehčíte pracovní zátěže zálohy, musí být tento soubor instalován na záložním serveru vStorage.	√	√

Tabulka 1. Dostupné komponenty produktu Data Protection for VMware podle operačního systému (pokračování)

Komponenta	Linux®	Windows
Data Protection for VMware vSphere Tato komponenta je grafické uživatelské rozhraní (GUI), které přistupuje k datům virtuálního počítače na serveru VMware vCenter. Obsah grafického rozhraní je k dispozici v těchto pohledech: • Pohled webového prohlížeče. Tento pohled je zpřístupněn webovým prohlížečem pomocí adresy URL pro hostitele webového serveru grafického rozhraní. Například: `https://guihost.mycompany.com:9081/TsmVMwareUI/` • Pohled IBM Spectrum Protect vSphere Client plug-in. K tomuto pohledu přistoupíte ve webovém klientovi VMware vSphere. Panely v tomto pohledu jsou jedinečně navrženy tak, aby se integrovaly do webového klienta vSphere, ale data a příkazy pro tento pohled jsou získávány ze stejného webového serveru grafického rozhraní jako ostatní pohledy. Modul IBM Spectrum Protect vSphere Client plug-in poskytuje dílčí sadu funkcí, které jsou k dispozici v pohledu webového prohlížeče, a některé další funkce.	√	√
Grafické rozhraní obnovy souborů Tato komponenta je grafické rozhraní založené na webu, které vám umožní obnovit soubory ze zálohy virtuálního počítače VMware bez pomoci administrátora. Grafické rozhraní je nainstalováno automaticky při instalaci grafického rozhraní produktu Data Protection for VMware. Je povoleno pomocí průvodce konfigurací.	√	√
Modul pro přesouvání dat Modul pro přesouvání dat IBM Spectrum Protect Data Protection for VMware je komponenta, která přesouvá data pro produktu Data Protection for VMware. Modul pro přesouvání dat přesouvá data z virtuálního prostředí na záložní server IBM Spectrum Protect. Při instalaci modulu pro přesouvání dat na server lze tento server použít jako záložní server vStorage. Modul pro přesouvání dat můžete nainstalovat na stejný systém jako produkt Data Protection for VMware nebo na jiný server. Pevné umístění instalace na systému Windows: `C:\Program Files\Tivoli\TSM\baclient`	√	√

Prostředí JVM je na systému Windows nainstalováno v: `C:\Program Files\Common Files\Tivoli\TSM\jvmNNNNNN`, kde `NNNNNN` je číslo verze prostředí JVM (například `JVM80516`). Webový server je nainstalovaný v `C:\IBM\SpectrumProtect\webserver`.

Počínaje verzí Data Protection for VMware 8.1.8 a novější nelze nadále změnit umístění komponent Framework a DP for VMware balíku TSM4VE. Výchozí umístění je `C:\Program Files\IBM\SpectrumProtect`.

- Framework - `C:\Program Files\IBM\SpectrumProtect\Framework`: soubory FLR, Derby, vmcli a tsmcli.
- DP for VMware - `C:\Program Files\IBM\SpectrumProtect\DPVMware`: soubory vmgui.

1. Přestože komponenta rozhraní pro obnovu souborů musí být nainstalována a povolena v systému Windows, můžete toto rozhraní použít k obnově souborů jak pro virtuální počítače hostované na systému Windows, tak i Linux.
2. Když nainstalujete produkt Data Protection for VMware, modul pro přesouvání dat je zahrnut v instalaci.

Produkt Data Protection for VMware odkládá pracovní zátěž zálohy z virtuálních počítačů na záložní server nástroje vStorage. Modul pro přesouvání dat musí být instalovaný na záložním serveru vStorage, aby bylo možné dokončit tuto úlohu.

Data Protection for VMware vSphere

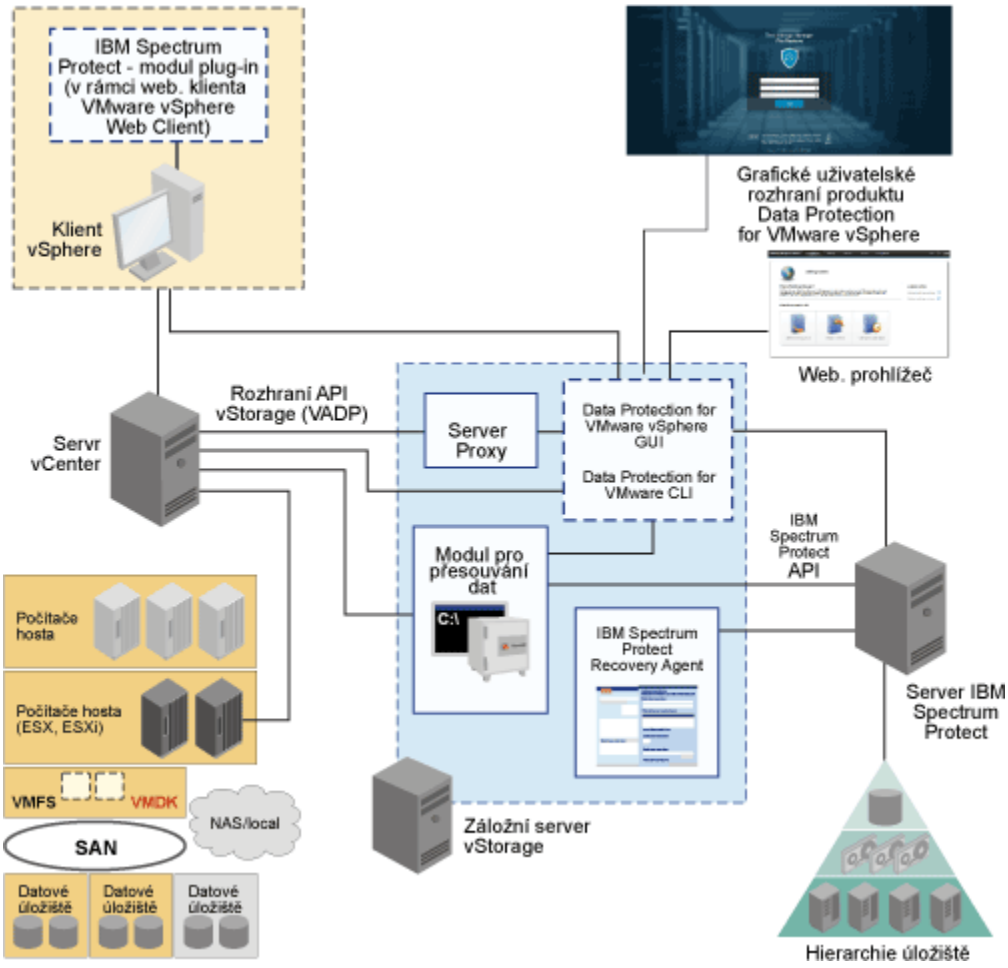
Grafické rozhraní produktu Data Protection for VMware vSphere (grafické rozhraní vSphere) je grafické uživatelské rozhraní, které přistupuje k datům virtuálního počítače na serveru VMware vCenter Server.

Přehled

Grafické rozhraní produktu Data Protection for VMware vSphere je primární rozhraní, ze kterého provedete následující úlohy:

- Zahájit nebo naplánovat zálohy virtuálních počítačů na server IBM Spectrum Protect.
- Zahájit úplnou obnovu vašich virtuálních počítačů ze serveru IBM Spectrum Protect.
- Vykázat sestavy o průběhu úloh, nejnovějších dokončených událostí, stavů záloh a využití prostoru. Tyto informace vám mohou pomoci při odstraňování chyb, ke kterým došlo ve zpracování zálohy.

Tip: Informace o tom, jak provádět úlohy pomocí grafického uživatelského rozhraní služby vSphere jsou poskytnuty v nápovědě online, která je nainstalována s grafickým rozhraním. Klepnutím na volbu **Další informace** v kterémkoli z oken grafického rozhraní otevřete nápovědu online pro podporu s úlohami.



Obrázek 1. Komponenty systému Data Protection for VMware v uživatelském prostředí VMware vSphere

Požadavky

Grafické rozhraní produktu Data Protection for VMware vSphere může být nainstalováno na libovolném systému splňujícím předpoklady operačního systému. Požadavky na prostředky grafického rozhraní vSphere jsou minimální, poněvadž nezpracovává přenosy dat I/O.

Tip: Instalace grafického rozhraní vSphere na záložní server vStorage je nejběžnější konfigurací.

Grafické rozhraní vSphere musí mít síťovou konektivitu k následujícím systémům:

- záložní server vStorage
- server IBM Spectrum Protect
- server vCenter

Kromě toho musí být k dispozici porty pro databázi Derby (výchozí 1527) a webový server grafického rozhraní (výchozí 9081).

Konfigurace

Můžete registrovat více grafických rozhraní vSphere na jediný server vCenter. Tento scénář snižuje počet datových středisek (a jejich hostitelských záloh virtuálních počítačů) spravovaných jediným grafickým rozhraním produktu VMware vSphere. Server vCenter pak může spravovat podmnožinu z celkového počtu datových středisek definovaných na Serveru vCenter.

Chcete-li aktualizovat spravovaná datová střediska, přejděte do nabídky **Konfigurace** > **Upravit konfiguraci**.

Při registraci několika grafických rozhraní vSphere na jediný server vCenter Server platí následující pokyny:

- Každé datové středisko může být spravováno pouze jedním instalovaným grafickým rozhraním vSphere.
- Pro každé instalované grafické rozhraní vSphere je požadovaný jedinečný název uzlu VMCLI.
- Použití jedinečných názvů uzlu modulu pro přesouvání dat pro každé nainstalované grafické rozhraní vSphere zjednodušuje správu uzlů.

Přístup ke grafickému rozhraní produktu vSphere

Ke grafickému rozhraní vSphere lze přistupovat těmito metodami:

- Samostatné grafické rozhraní webového prohlížeče. K tomuto grafickému rozhraní se přistupuje pomocí záložky adresy URL na webový server grafického rozhraní, například:

  ```
  https://název_hostitele:port/TsmVMwareUI/
  ```

  kde:

  – *název_hostitele* je název systému, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere

  – *port* je číslo portu, na kterém je k přístupné grafické rozhraní vSphere. Výchozí číslo portu je 9080. Pro zabezpečené porty je výchozí hodnota 9081.
- Rozšíření webového klienta vSphere, které se připojí k webovému serveru grafického rozhraní pro přístup k virtuálním počítačům v úložišti IBM (označované jako rozšíření ochrany dat). Obsah je podmnožinou toho, co je poskytováno v grafickém rozhraní webového prohlížeče.

Během instalace můžete uvést jednu nebo více přístupových metod.

Windows Výchozí instalační adresář je `C:\IBM\SpectrumProtect\webserver`.

Linux Výchozí instalační adresář je `/opt/tivoli/tsm/tdpvmware/common/webserver`.

Agent zotavení produktu IBM Spectrum Protect

Pro připojení libovolného svazku snímků ze serveru IBM Spectrum Protect použijte službu agenta zotavení.

Přehled

Můžete použít protokol iSCSI pro přístup ke snímku ze vzdáleného systému.

Potřebujete-li si snímky zobrazit lokálně na klientském systému (v režimu pouze pro čtení), použijte produkt Data Protection for VMware V8.1.4 či předchozí verze.

Navíc agent zotavení poskytuje produkt funkci okamžité obnovy a ochranu pro hostované aplikace. Okamžitá obnova povolí svazku, který je používán, zůstat v dostupném stavu během operace obnovy, která pokračuje v pozadí. Ochrana aplikací umožňuje aplikacím instalovaným na virtuálním počítači hosta, jako je Microsoft Exchange Server a Microsoft SQL Server, aby byly k dispozici pro ochranu zálohování a obnovy.

Agent zotavení může dokončit následující úlohy ze vzdáleného systému:

- Shromážděte informace o datech, které lze obnovit, například:
  – Zálohované virtuální počítače.
  – Snímky dostupné pro zálohované virtuální počítače.
  – Oblasti dostupné ve specifickém snímku.

Podrobné informace o příkazech, parametrech a návratových kódech naleznete v sekci s popisem příkazů v uživatelské příručce *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide*.

Požadavky

Windows Na systémech Windows je grafické uživatelské rozhraní i rozhraní příkazového řádku agenta zotavení instalováno v rámci úplné instalace produktu Data Protection for VMware nebo v rámci rozšířené instalace modulu pro přesouvání dat.

Přístup k agentovi zotavení

Windows K agentovi zotavení můžete přistoupit z nabídky **Start**: **Start** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **Agent zotavení IBM Spectrum Protect**

IBM Spectrum Protect vSphere Client plug-in

Modul IBM Spectrum Protect vSphere Client plug-in je rozšíření webového klienta VMware vSphere, které poskytuje pohled na grafické rozhraní produktu Data Protection for VMware vSphere.

Přehled

Modul IBM Spectrum Protect vSphere Client plug-in poskytuje dílčí sadu funkcí, které jsou k dispozici v zobrazení prohlížeče pro grafické rozhraní produktu Data Protection for VMware vSphere a některé další funkce.

Požadavek

Chcete-li nainstalovat modul IBM Spectrum Protect vSphere Client plug-in, musíte vybrat následující volby, když spustíte průvodce konfigurací produktu IBM Spectrum Protect for Virtual Environments:

- Na stránce **Nastavení služby vCenter** v průvodci konfigurací vyberte volbu **Aktualizovat registraci**, abyste registrovali modul plug-in v přidružené službě vCenter.
- Zadejte adresu hostitele grafického rozhraní, uživatele a heslo služby vCenter.

  Poznámka: Výchozí doména je založena na adrese lokální domény a nemusí být externí přístupná. Je-li požadován externí přístup, uveďte adresu hostitele grafického rozhraní, kterou lze interpretovat pomocí DNS nebo adresy IP.

Po dokončení průvodce bude modul plug-in registrován ve službě vCenter.

Přístup k modulu plug-in ochrany dat

K modulu plug-in můžete přistoupit z webového klienta vSphere:

1. Přihlaste se k webovému klientovi vSphere pomocí pověření služby vCenter. Modul plug-in ochrany dat se nachází pod hlavní nabídkou, **IBM Spectrum Protect**.
2. Výběr této položky nabídky vás přenese do hlavní oblasti rozšíření produktu IBM Spectrum Protect. Sekce **Monitorovat** a **Konfigurovat**, které jsou přidružené ke konkrétním položkám soupisu služby vCenter, budou mít rovněž funkce produktu IBM Spectrum Protect for Virtual Environments.

Komponenta rozhraní příkazového řádku produktu Data Protection for VMware

Komponenta rozhraní CLI produktu Data Protection for VMware je plně funkční rozhraní příkazového řádku nainstalované s grafickým rozhraním produktu Data Protection for VMware vSphere.

Přehled

Pomocí rozhraní CLI produktu Data Protection for VMware můžete provést tyto úlohy:

- Zahájit nebo naplánovat zálohy virtuálních počítačů na server IBM Spectrum Protect.
- Zahájit úplnou obnovu vašich virtuálních počítačů, souborů virtuálních počítačů nebo disků virtuálních počítačů (VMDK) ze serveru IBM Spectrum Protect.
- Zobrazit informace o konfiguraci databáze a prostředí zálohy.

Ačkoli je grafické rozhraní produktu Data Protection for VMware vSphere primárním rozhraním úlohy, rozhraní CLI produktu Data Protection for VMware poskytuje užitečné sekundární rozhraní.

Komponentu rozhraní CLI produktu Data Protection for VMware lze například použít k implementaci mechanismu plánování, který je odlišný od toho, který je implementován grafickým rozhraním produktu Data Protection for VMware vSphere. Komponenta rozhraní CLI produktu Data Protection for VMware je také užitečná při vyhodnocení výsledků automatizace se skripty.

Přístup k rozhraní příkazového řádku produktu Data Protection for VMware

Ke komponentě rozhraní CLI produktu Data Protection for VMware můžete přistoupit z příkazového řádku.

Podrobné informace o dostupných příkazech viz sekce s popisem příkazů v uživatelské příručce *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide*

Rozhraní pro obnovu souborů produktu IBM Spectrum Protect

Můžete obnovit jednotlivé soubory ze zálohování virtuálních počítačů VMware.

Přehled

Rozhraní obnovy souborů je rozhraní založené na webu, kde můžete obnovit jednotlivé soubory ze zálohy virtuálního počítače. Výhodou tohoto rozhraní je, že vlastníci souboru, softwaru a platformy mohou obnovit své vlastní soubory bez předchozí znalosti operací zálohy a obnovy produktu IBM Spectrum Protect.

Funkce rozhraní obnovy souborů se nainstaluje, když vyberete volbu ochránit data v prostředí vSphere. V průvodci konfigurací Data Protection for VMware musíte povolit funkci obnovy souboru, aby bylo rozhraní k dispozici.

Přístup k rozhraní pro obnovu souborů produktu IBM Spectrum Protect

Chcete-li získat přístup k rozhraní pro obnovu souborů, otevřete webový prohlížeč a zadejte adresu URL, kterou vám poskytl administrátor. Například:

```
https://hostname:9081/FileRestoreUI
```

kde *hostname* je název hostitele systému, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere.

Funkce modulu pro přesouvání dat

Modul pro přesouvání dat je softwarová komponenta produktu Data Protection for VMware, která přesouvá data na a ze serveru Server IBM Spectrum Protect.

Přehled

V typickém prostředí VMware se modul pro přesouvání dat používá k uložení záloh virtuálního počítače do uzlu datového střediska.

Když nainstalujete produkt Data Protection for VMware, modul pro přesouvání dat je zahrnut v instalaci. Modul pro přesouvání dat je nainstalován na stejném systému jako grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere a další komponenty produktu Data Protection for VMware.

Chcete-li přerozdělit pracovní zátěž zálohování mezi více systémů, můžete také instalovat moduly pro přesouvání dat na vzdálené systémy nezávisle na dalších komponentách produktu Data Protection for VMware.

Operace rozdílové zálohy snímků nejsou podporovány v prostředí VMware. Nemůžete spustit operace rozdílové zálohy snímků pro systém souborů, který sídlí v úložišti NetApp na hostiteli, kde je také nainstalován modul pro přesouvání dat produktu Data Protection for VMware.

Nastavení modulů pro přesouvání dat

Prohlédněte si informace o plánování, instalaci a konfiguraci modulu pro přesouvání dat v tomto seznamu:

Akce	Popis
Určete počet modulů pro přesouvání dat požadovaných k ochraně prostředí vSphere.	K ochraně prostředí vSphere může být požadováno více uzlů modulu pro přesouvání dat. Chcete-li určit počet požadovaných uzlů modulu pro přesouvání dat, prohlédněte si technickou poznámku 2007197. Tato technická poznámka také obsahuje pokyny pro používání virtuálních nebo fyzických počítačů pro uzly a lokalitu modulu pro přesouvání dat.
Nainstalujte produkt Data Protection for VMware.	Chcete-li nainstalovat produkt Data Protection for VMware, spusťte instalační program produktu Data Protection for VMware a vyberte volbu **Typická instalace** pro operační systémy Windows nebo **Úplná** pro operační systémy Linux. Tato volba instalace nainstaluje všechny komponenty produktu Data Protection for VMware včetně modulu pro přesouvání dat. Informace o způsobu spuštění instalačního programu produktu Data Protection for VMware naleznete v sekci “Instalace komponent produktu Data Protection for VMware” na stránce 20.
Nadefinujte moduly pro přesouvání dat pro vaše prostředí.	Po dokončení průvodce instalací produktu Data Protection for VMware se otevře průvodce konfigurací grafického rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere a umožní vám nastavit komunikaci s komponentou Server IBM Spectrum Protect. Na stránce **Uzly modulu pro přesouvání dat** v průvodci konfigurací definujte informace o lokálním modulu pro přesouvání dat a jakýchkoli vzdálených modulech pro přesouvání dat, které budete instalovat na oddělené systémy. Jestliže instalujete na operační systém Windows a při definování modulu pro přesouvání dat vyberete volbu **Vytvořit služby**, uloží se informace o konfiguraci modulu pro přesouvání dat do souboru voleb v tomto umístění: `C:\Program Files\Tivoli\TSM\baclient\` Kromě toho se nakonfigurují služby, které modul pro přesouvání dat požaduje. Pokud nainstalujete modul pro přesouvání dat na operační systém Linux nebo na operační systém Windows, ale nevyberete během konfigurace volbu **Vytvořit služby**, musíte provést postup v sekci “Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere” na stránce 83, abyste vytvořili soubor voleb a nakonfigurovali požadované služby.

Akce	Popis
Podle potřeby nainstalujte a nakonfigurujte další moduly pro přesouvání dat na vzdálených systémech.	Chcete-li nainstalovat modul pro přesouvání dat na vzdáleném systému, spusťte instalační program produktu Data Protection for VMware a proveďte jednu z těchto akcí: Na operačních systémech Windows vyberte v průvodci konfigurací volby **Rozšířená instalace** > **Instalovat pouze funkci modulu pro přesouvání dat**. Na operačních systémech Linux vyberte v průvodci konfigurací volbu **Vlastní** ze seznamu **Instalační sada**. Ujistěte se, že je vybraná položka **Modul pro přesouvání dat produktu Data Protection for VMware**. Tato volba se vybere standardně. Po dokončení instalace postupujte podle pokynů v sekci “Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere” na stránce 83, abyste nastavili moduly pro přesouvání dat na vzdálených systémech.

Plánování instalace produktu Data Protection for VMware

Produkt Data Protection for VMware eliminuje vliv spuštěných záloh na virtuální počítač odlehčením pracovní zátěže zálohy z hostitele založeného na VMware ESXi na záložní server vStorage.

Produkt Data Protection for VMware funguje s integrovaným modulem pro přesouvání dat a provádí trvale přírůstková úplná a přírůstková zálohování virtuálních počítačů. Uzel modulu pro přesouvání dat "přesouvá" data na server IBM Spectrum Protect, kde jsou uložena, a později se virtuální počítač obnoví na úrovni obrazu. Okamžitá obnova je k dispozici na úrovni diskového svazku a na úrovni úplného virtuálního počítače.

Tip: Modul pro přesouvání dat je odděleně licencovaná komponenta obsahující vlastní uživatelská rozhraní a dokumentaci. Chcete-li adekvátně integrovat souhrnný plán pro ochranu vašich virtuálních počítačů pomocí produktu Data Protection for VMware, je nezbytná znalost tohoto produktu a jeho dokumentace. Produkt Data Protection for VMware pro 64bitový systém Windows zahrnuje funkci modulu pro přesouvání dat.

Orientační plán instalace

Následující tabulka uvádí kroky pro dokončení úspěšného instalačního procesu.

Tabulka 2. Instalační úlohy pro nové nebo existující zákazníky produktu Data Protection for VMware

Krok	Úloha	Začněte zde
1	Zkontrolujte požadavky na systém.	Ujistěte se, že systém, na který se má nainstalovat produkt Data Protection for VMware, splňuje systémové požadavky.
2	Zkontrolujte požadavky na oprávnění uživatele.	Vyvarujte se chyb instalace nebo prodlev pomocí požadovaných úrovní oprávnění uživatele.
3	Zkontrolujte dostupnost požadovaných komunikačních portů.	Vyvarujte se chyb instalace nebo prodlev otevřením požadovaných komunikačních portů, než se pokusíte nainstalovat produkt Data Protection for VMware.

Tabulka 2. Instalační úlohy pro nové nebo existující zákazníky produktu Data Protection for VMware (pokračování)

Krok	Úloha	Začněte zde
4	Nainstalujte produkt Data Protection for VMware: • Instalace produktu Data Protection for VMware pomocí průvodce instalací • "Instalace komponent produktu Data Protection for VMware v bezobslužném režimu" na stránce 24 Upgrade produktu Data Protection for VMware: Upgrade produktu Data Protection for VMware	Každý balík instalace vám zobrazí soubor s uživatelskou licencí (EULA). Pokud soubor nepřijmete, instalace je ukončena.
5	"Konfigurace nové instalace v průvodci na systému Windows" na stránce 39 Pokud plánujete upgradovat produkt Data Protection for VMware, může být nezbytné provedení dalších konfiguračních úloh v závislosti na instalovaných komponentách. Další informace naleznete v tématech o konfiguraci v uživatelské příručce *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide*.	Pro počáteční konfiguraci použijte průvodce konfigurací. V závislosti na funkcích, které jsou nainstalovány, může být požadováno více konfiguračních úloh, jak popisuje tato sekce.

Tip: K usnadnění plánování množství hostitelů serveru proxy požadovaných pro vaše specifické prostředí zálohy produktu Data Protection for VMware je k dispozici na wikiwebu IBM Spectrum Protect následující publikace:
Podrobná příručka pro dimenzování záložního serveru vStorage (Proxy)
Tato příručka je k dispozici v sekci produktu IBM Spectrum Protect for Virtual Environments.

Scénáře instalace

Než nainstalujete produkt Data Protection for VMware, vyberte si scénář, který nejlépe vyhovuje vašim obchodním potřebám.

Můžete nainstalovat produkt Data Protection for VMware a modul pro přesouvání dat pomocí grafického rozhraní nebo v bezobslužném režimu:

- "Instalace komponent produktu Data Protection for VMware pomocí průvodce instalací" na stránce 21
- "Instalace komponent produktu Data Protection for VMware v bezobslužném režimu" na stránce 24

Chcete-li získat seznam funkcí a komponent, které jsou k dispozici podle platformy, prohlédněte si sekci "Instalovatelné komponenty" na stránce 1.

Tabulka 3. Scénáře instalace		
Číslo scénáře	**Popis**	**Úlohy, které musíte provést**
1	Tento scénář použijte pro novou instalaci, kde budete chtít nainstalovat produkt Data Protection for VMware a modul pro přesouvání dat na stejný systém.	Windows Můžete použít instalační program sady v grafickém rozhraní nebo v bezobslužném režimu. Linux Můžete použít instalační program v grafickém rozhraní nebo v bezobslužném režimu.
2	Pomocí tohoto scénáře nainstalujte modul pro přesouvání dat (server proxy pro připojení), agenta zotavení a požadované balíky podpory na tomto systému.	Windows Rozšířenou instalaci můžete dokončit pomocí instalačního programu sady. Linux Funkce modulu pro přesouvání dat je nyní nainstalována spolu s produktem Data Protection for VMware.

Systémové požadavky

Chcete-li implementovat komponenty Data Protection for VMware, váš systém musí splňovat odpovídající požadavky na systém.

Požadavky na software

Podrobnosti požadavků na software a operační systém se mohou časem změnit. Aktuální požadavky na software viz technická poznámka 1505139.

Hardwarové požadavky

Hardwarové požadavky se liší a závisí na následujících položkách:

- počet chráněných serverů
- počet chráněných svazků
- velikosti datových sad
- konektivita sítí LAN a SAN

Poznámka: Agent zotavení nepodporuje operace v prostředí mimo síť LAN.

Následující tabulka popisuje hardwarové požadavky potřebné k instalaci produktu Data Protection for VMware.

Tabulka 4. Hardwarové požadavky produktu Data Protection for VMware.		
Komponenta	**Minimální požadavek**	**Upřednostňováno**
Systém	Procesor IntelPentium D Dual Core nebo kompatibilní	Nelze aplikovat
Paměť	4 GB RAM, 4 GB virtuálního adresního prostoru	Nelze aplikovat
Dostupný pevný disk	4.4 GB	9.0 GB
Síť	1 GbE	10 GbE

Poznámka: V závislosti na počtu paralelních procesů vyžadují zálohy virtuálních počítačů značné množství paměti.

Požadavky na paměť vzhledem k příkazu **dsmc backup vm** je možné rozbalit a vypočítat pomocí následujícího vzorce:

Požadovaná paměť = (DiskSize / MBLKSize) * ReadBufferSize * VMMAXPARALLEL

kde:

- **DiskSize** je velikost disku hosta, který se momentálně zpracovává.
- **MBLKSize** je velikost megabloku. Hodnota je rovna 128 MB pro disky pod 2 TB a 1 GB pro disky větší než 2 TB.
- **ReadBufferSize** je velikost vnitřní vyrovnávací paměti produktu IBM Spectrum Protect, která se použije k uložení informací o megabloku. Velikost vyrovnávací paměti se rovná 256 KB.
- **VMMAXPARALLEL** je maximální počet virtuálních počítačů, které lze kdykoli zálohovat pomocí jednoho procesu operace zálohování.

Například, chcete-li zálohovat 10 hostů, každý s disky o 40 GB, a spustit VMMAXPARALLEL 2 v rámci jednoho procesu operace zálohování, budete potřebovat:

- **DiskSize** = 40 GB = 41943040 KB
- **MBLKSize** = 128 MB = 131072 KB
- **ReadBufferSize** = 256 KB
- **VMMAXPARALLEL** = 2

Požadovaná paměť = (41943040 / 131072) * 256kB * 2 = 163840KB = 160MB.

Poznámka: Aby bylo možné zálohovat stejný počet hostů s pomocí 'VMMAXPARALLEL 2' v pěti paralelních procesech operace zálohování, bylo by potřeba (maximálně) pětkrát více paměti než v předchozím příkladu, nebo 800 MB.

Omezení: Následující omezení se vztahují jen na disky VMware VMDK, které jsou zahrnuty do operace zálohy:

- Pro režim trvalé přírůstkové zálohy nesmí žádný jednotlivý disk VMDK zahrnutý do operace zálohy překračovat 8 TB. Pokud disk VMDK překročí 8 TB, operace zálohy selže. Chcete-li zvýšit velikost disku VMDK na hodnu vyšší, než je předvolba 2 TB, uveďte maximální velikost pomocí volby `vmmaxvirtualdisks`. Chcete-li získat další informace, vyhledejte `vmmaxvirtualdisks` v Centru znalostí IBM.

Chcete-li zabránit selhání během kteréhokoli režimu zálohování, můžete přeskočit zpracování disku VMDK uvedením volby `vmskipmaxvirtualdisks yes` v souboru voleb modulu pro přesouvání dat. Další informace viz téma Vmskipmaxvirtualdisks.

Nezbytné předpoklady obnovy souboru

Než obnovíte soubory pomocí rozhraní pro obnovu souborů produktu IBM Spectrum Protect Data Protection for VMware, ujistěte se, že vaše prostředí splňuje minimální předpoklady.

Chcete-li povolit funkci obnovy souborů, na systému Windows musí být nainstalován produkt Data Protection for VMware.

Nezbytné předpoklady virtuálního počítače VMware

Následující nezbytné předpoklady se týkají virtuálního počítače VMware, který obsahuje soubory pro obnovení:

- Windows Linux Nástroje VMware Tools musí být nainstalovány na virtuálním počítači.
- Windows Linux Virtuální počítač musí být spuštěn během operace obnovy souborů.
- Windows Systém modulu pro přesouvání dat musí buď náležet do stejné domény systému Windows, nebo musí být v doméně se vztahem důvěryhodnosti s virtuálním počítačem obsahujícím soubory, které mají být obnoveny.
- Windows Když se virtuální počítač odstraní z domény systému Windows a později se obnoví, virtuální počítač musí být opět přidán do domény, aby byl zajištěn vztah důvěryhodnosti domény. Nepokoušejte se provést obnovu souborů z virtuálního počítače, dokud není obnoven vztah důvěryhodnosti domény.

- Windows Pokud uživatel není vlastníkem souboru, který má být obnoven, oprávnění systému Microsoft Windows `Obnovit soubory a adresáře` musí být uživateli přiřazeno pro daný virtuální počítač.
- Další informace o předpokladech účtu domény Microsoft Windows vyžadovaných pro použití rozhraní pro obnovu souborů produktu Data Protection for VMware naleznete v technické poznámce 1998066.
- Linux Pro virtuální počítač je požadováno ověření lokálního uživatele. Ověření není dostupné přes doménu systému Windows, protokol LDAP (Lightweight Directory Access Protocol), Kerberos nebo jiné síťové metody ověření.
- Linux Na operačním systému Red Hat Enterprise Linux 6 musí volba `ChallengeResponseAuthentication` ov konfiguračním souboru démona sshd (`/etc/ssh/sshd_config`) uvádět ANO nebo musí být označena jako komentář. Platné jsou například oba z následujících příkazů:

  ```
  ChallengeResponseAuthentication yes
  ```

  ```
  #ChallengeResponseAuthentication no
  ```

  Restartujte démona sshd po úpravě této volby.

Nezbytné předpoklady modulu pro přesouvání dat

Systém modulu pro přesouvání dat představuje specifický modul pro přesouvání dat, který "přesouvá data" z jednoho systému na druhý.

Windows Systém modulu pro přesouvání dat musí patřit do stejné domény Windows jako virtuální počítač, který obsahuje soubory pro obnovení.

Nezbytné předpoklady serveru proxy pro připojení

Systém serveru proxy pro připojení představuje systém serveru proxy Linux nebo Windows, který přistupuje k připojeným diskům virtuálních počítačů pomocí připojení iSCSI. Tento systém umožňuje, aby byly systémy souborů na připojených discích virtuálních počítačů přístupné jako body obnovy pro rozhraní pro obnovu souborů.

Linux Operační systémy Linux poskytují démona, který aktivuje skupiny svazku LVM, jak se tyto skupiny stávají dostupnými pro tento systém. Nastavte tohoto démona na systému Linux serveru proxy pro připojení tak, aby skupiny svazků LVM nebyly aktivovány, jakmile se stanou přístupnými pro systém. Podrobné informace o tom, jak nastavit tohoto démona viz odpovídající dokumentace systému Linux.

Windows Linux Systém Windows serveru proxy pro připojení a systém Linux servery proxy pro připojení musí být na stejné podsíti.

Nezbytné předpoklady pro účet domény systému Microsoft Windows

Následující nezbytné předpoklady se vztahují na účty domény systému Windows. První požadavek je zavést uživatelský účet domény Windows s lokálním administrativním oprávněním na všech virtuálních počítačích:

- Chcete-li provést nezbytné úlohy, abyste povolili obnovu souborů pro hosta virtuálního počítače, potřebujete uživatelský účet, který patří doméně Windows a je lokální administrátor v systému serveru proxy pro připojení. Administrátor s tímto účtem zadá pověření účtu do průvodce konfigurací grafického rozhraní produktu Data Protection for VMware vSphere nebo do zápisníku, aby povolil prostředí pro operace obnovy souborů.
- Chcete-li vytvořit uživatelský účet s dostatečnými oprávněními pro používání souborů rozhraní pro obnovu souborů, můžete pomocí objektu zásad skupiny Windows centrálně spravovat jednotlivého uživatele domény, umožnit přístup k více počítačům s pověřeními lokálního administrátora a případně omezit nežádoucí akce.

Následující kroky ukazují, jak lze tento uživatelský účet vytvořit. Na řadiči domény pomocí modulu snap-in MMC počítačů a uživatelů služby Active Directory postupujte takto:

1. Vyberte nabídku **Akce->Nový->Skupiny** a vytvořte novou skupinu zabezpečení s názvem **FR Admins**. Rozsah skupiny by měl být nastaven na `Globální`.
2. Vytvořte nový uživatelský účet domény se jménem uživatele `frcmin1` a přidejte jej do skupiny zabezpečení **FR Admins**. Můžete také přidat další účty uživatelů domény do skupiny.
3. Chcete-li poskytnout větší kontrolu nad sadou počítačů, ke kterým má `fradmin1` přístup, vytvořte novou organizační jednotku.
4. Z objektu domény vyberte nabídku **Nový->Organizační jednotka** a pojmenujte ji `FR Computers`.
5. Naplňte organizační jednotku `FR Computers` řadou počítačů. .

Dokončete následující kroky na řadiči domény z modulu snap-in MMC zásady skupiny:

1. Vytvořte nový objekt zásady skupiny s názvem `FR Admin GPO`, který přidá administrátory do skupiny **FR Admins** do skupiny lokálních administrátorů počítačů přidružených k organizační jednotce, na kterou se vztahuje objekt zásady skupiny.
2. V objektu zásady skupiny přidejte účet do skupiny lokálních administrátorů a volitelně do vzdálených uživatelů počítače.
3. Vyberte organizační jednotku `FR Computers` a přidejte nově vytvořený objekt zásady skupiny.

   Poznámka: Objekt zásad skupiny mohl být přidružen k samotné doméně, ale pak by `fradmin1` měl patřit do skupiny lokálních administrátorů pro všechny počítače v doméně. Použití explicitní organizační jednotky poskytuje další řízení.
4. Volitelně: použijte správu zásad skupiny k omezení nežádoucích akcí na lokálním počítači, jako je `Odepřít přihlášení lokálně` a `Odepřít přihlášení přes Terminal Services`.
5. Na stránce Obnova souboru průvodce konfigurací grafického rozhraní produktu Data Protection for VMware vSphere nebo zápisníku aktualizujte nastavení pro použití účtu `domain\fadmin1`, který byl vytvořen ve výše uvedených krocích.
6. Restartujte službu démon Client Access Daemon (CAD) serveru proxy pro připojení.

Po nastavení účtu s vhodnými oprávněními:

- Windows Zadejte svá pověření v průvodci konfigurací grafického rozhraní produktu Data Protection for VMware vSphere nebo zápisníku, abyste povolili prostředí pro operace obnovy souborů.
- Windows Vlastník souboru přistupuje ke vzdálenému virtuálnímu počítači (který obsahuje soubory, jež mají být obnoveny) s pověřením uživatele domény Windows. Tato pověření jsou zadána do rozhraní pro obnovu souborů během přihlášení. Oprávnění uživatele domény, ke které má vlastník souboru oprávnění se přihlásit na vzdálený virtuální počítač a obnovit soubory do tohoto vzdáleného virtuálního počítače. Tato pověření nevyžadují žádná speciální oprávnění.
- Windows Pokud vlastník souboru využívá účet uživatele domény Windows, který omezuje přístup ke specifickým počítačům (namísto přístupu ke všem počítačům v doméně), ujistěte se, že je systém serveru proxy pro připojení zahrnut v seznamu počítačů, které jsou přístupné pro tento uživatelský účet domény. Jinak se vlastník souboru nebude moci přihlásit do rozhraní pro obnovu souborů.

Nezbytné předpoklady páskových médií

Obnova souboru z páskového média není podporována. Obnova souboru z diskového úložiště je upřednostňovanou metodou.

Požadované oprávnění k instalaci

Než začnete s instalací, ujistěte se, že váš identifikátor uživatele obsahuje požadovanou úroveň oprávnění.

Informace o této úloze

Tabulka 5. Oprávnění uživatelů požadovaná pro instalaci a konfiguraci produktu Data Protection for VMware

Systém	**Povinné oprávnění**
Windows	Administrátor
Linux	Kořen
Server vCenter	Oprávnění administrátora Role serveru vCenter vyžaduje následující oprávnění: **Rozšíření** > **Registrovat rozšíření, Zrušit registraci rozšíření, Aktualizovat rozšíření** Tato nová role musí být aplikována na objekt vCenter v hierarchii serveru VMware vCenter pro ID uživatele uvedeného během instalace.
Server IBM Spectrum Protect **Omezení:** Server musí být spuštěn.	Administrativní přístup (Oprávnění **Systém** nebo **Neomezená doména zásad**)

Požadované komunikační porty
Zobrazení seznamu komunikačních portů, které musí být otevřeny v bráně firewall při instalaci produktu Data Protection for VMware.

Porty, které jsou identifikovány v tabulce, odráží typickou instalaci. Typická instalace se skládá z následujících komponent na stejném systému Windows:

- server grafického rozhraní Data Protection for VMware
- záložní server vStorage (modul pro přesouvání dat)
- server proxy připojení Windows
- rozhraní pro obnovu souborů produktu IBM Spectrum Protect

V případě netypické instalace mohou být vyžadovány další porty.

Omezení: Server proxy připojení systému Windows a server proxy připojení systému Linux musí být na stejné podsíti.

Tabulka 6. Požadované komunikační porty. Tato tabulka identifikuje porty, ke kterým může přistupovat produkt Data Protection for VMware.

Port TCP	**Iniciátor: Odchozí (Z hostitele)**	**Cíl: Příchozí (Hostiteli)**
443	Záložní server vStorage	Server vCenter (zabezpečený protokol HTTP)
443	Grafické rozhraní produktu Data Protection for VMware vSphere Server	Server vCenter
443 Toto nastavení je požadováno jen tehdy, pokud je modul pro přesouvání dat na systému Linux.	Server proxy připojení Windows	Server vCenter
443	Záložní server vStorage	Platform Services Controller

Tabulka 6. Požadované komunikační porty. Tato tabulka identifikuje porty, ke kterým může přistupovat produkt Data Protection for VMware. *(pokračování)*

Port TCP	Iniciátor: Odchozí (Z hostitele)	Cíl: Příchozí (Hostiteli)
443	Grafické rozhraní produktu Data Protection for VMware vSphere Server	Platform Services Controller
443	Server proxy připojení Windows	Platform Services Controller
902 443	Server vCenter	Hostitelé ESXi
902 443	Záložní server vStorage (server proxy)	Hostitelé ESXi (všechny chráněné hostitelské systémy)
1500 (**tcpport**)	Záložní server vStorage (server proxy)	Server IBM Spectrum Protect
1500 (**tcpadminport**)	Grafické rozhraní produktu Data Protection for VMware vSphere Server • 1500 (**tcpadminport**) je komunikace bez zabezpečení SSL • V případě komunikace SSL je **tcpadminport** jediný port, který podporuje komunikaci SSL se serverem IBM Spectrum Protect. Správné číslo portu, které se má použít pro protokol SSL, je obvykle hodnota uvedená volbou **ssltcpadminport** v souboru serveru IBM Spectrum Protect dsmserv.opt. Pokud je však uvedena volba **adminonclient no** v souboru dsmserv.opt, tak je správná hodnota portu, která se má použít pro protokol SSL, hodnota uvedená volbou **ssltcpadminport**. Volba **ssltcpadminport** nemá žádnou výchozí hodnotu. Proto ji musí uvést uživatel.	Server IBM Spectrum Protect
1527 Interní databáze Derby		
1501 1581 (**httpport**)	Server IBM Spectrum Protect	Záložní server vStorage • Plánovač modulu pro přesouvání dat • Webový klient • Démon Client Acceptor

Tabulka 6. Požadované komunikační porty. Tato tabulka identifikuje porty, ke kterým může přistupovat produkt Data Protection for VMware. *(pokračování)*

Port TCP	Iniciátor: Odchozí (Z hostitele)	Cíl: Příchozí (Hostiteli)
1581 (**httpport**) 1582, 1583 (**webports**)	Server Data Protection for VMware vSphere	Záložní server vStorage
9081 Webový server grafického rozhraní (protokol HTTPS)	Klient vSphere	Server grafického rozhraní produktu Data Protection for VMware vSphere (port zabezpečeného protokolu HTTPS pro přístup ke službě vCenter pomocí webového prohlížeče)
22 Výchozí port SSH pro agenta zotavení	Agent zotavení	Hostitel "připojení" Data Protection for VMware Windows • SSH pro agenta zotavení Linux
3260	Obnovení souboru v systému Linux Data Protection for VMware	Hostitel "připojení" Data Protection for VMware Windows • iSCSI
3260 Výchozí port iSCSI pro agenta zotavení	Cíl systému Windows s dynamickým diskem pro obnovu systému	Hostitel "připojení" Data Protection for VMware Windows • iSCSI
5985	Operace grafického rozhraní obnovy souborů	Vzdálená správa systému Windows
135	Server proxy připojení Windows	Virtuální počítač VMware obsahující soubory, které mají být obnoveny pomocí rozhraní pro obnovu souborů IBM Spectrum Protect

Požadavky na oprávnění uživatelů serveru VMware vCenter
Ke spuštění operací produktu Data Protection for VMware jsou zapotřebí jistá oprávnění serveru VMware vCenter.

Oprávnění serveru vCenter požadovaná k ochraně datových středisek VMware s pohledem webového prohlížeče pro grafické rozhraní produktu Data Protection for VMware vSphere

ID uživatele serveru vCenter Server, který se přihlásí do zobrazení prohlížeče, pro grafické rozhraní produktu Data Protection for VMware vSphere

musí mít dostateční oprávnění VMware k zobrazení obsahu datového střediska spravovaného grafickým rozhraním.

Prostředí VMware vSphere například obsahuje pět datových středisek. Uživatel, "jenn", má dostatečná oprávnění pouze pro dvě z těchto datových středisek. V důsledku toho jsou pouze tato dvě datová střediska, kde existují dostatečná oprávnění, pro uživatele "jenn" viditelná v pohledech. Ostatní tři datová střediska (kde uživatel "jenn" nemá oprávnění) nejsou pro tohoto uživatele viditelná.

Server VMware vCenter definuje sadu oprávnění společně jako roli. Role se použije na objekt pro určeného uživatele nebo určenou skupinu pro vytvoření oprávnění. Z webového klienta VMware vSphere

musíte vytvořit roli se sadou oprávnění. Chcete-li vytvořit roli serveru vCenter pro operace zálohy a obnovy, použijte funkci klienta VMware vSphere **Přidat roli**.

Chcete-li šířit oprávnění na všechna datová střediska v produktu vCenter, uveďte server vCenter a zaškrtněte zaškrtávací políčko `Šířit na podřízené prvky`. Jinak můžete omezit oprávnění, přiřadíte-li roli k požadovaným datovým střediskům výhradně se zaškrtnutým zaškrtávacím políčkem `Šířit na podřízené prvky`. Vynucení pro grafická rozhraní prohlížeče je na úrovni datového střediska.

Následující příklad ukazuje, jak řídit přístup k datovým střediskům pro dvě skupiny uživatelů VMware. Nejprve vytvořte roli, která obsahuje všechna oprávnění nadefinovaná v technické poznámce 7047438. Sada oprávnění v tomto příkladu je identifikována rolí nazvanou "TDPVMwareManage". Skupina 1 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska `Primary1_DC` a `Primary2_DC`. Skupina 2 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska `Secondary1_DC` a `Secondary2_DC`.

Pro skupinu 1 přiřaďte roli "TDPVMwareManage" k datovým střediskům `Primary1_DC` a `Primary2_DC`. Pro skupinu 2 přiřaďte roli "TDPVMwareManage" k datovým střediskům `Secondary1_DC` a `Secondary2_DC`.

Uživatelé v každé skupině uživatelů VMware mohou použít grafické rozhraní produktu Data Protection for VMware ke správě virtuálních počítačů pouze ve svých odpovídajících datových střediscích.

Tip: Když vytváříte roli, zvažte přidání dalších oprávnění do role, které můžete později potřebovat k dokončení jiných úloh na objektech.

Oprávnění serveru vCenter požadovaná pro použití modulu pro přesouvání dat

Modul pro přesouvání dat IBM Spectrum Protect, který je nainstalován na záložním serveru vStorage (uzel modulu pro přesouvání dat) vyžaduje volby `VMCUser` a `VMCPw`. Volba `VMCUser` uvádí ID uživatele serveru vCenter nebo ESX, který chcete zálohovat, obnovit nebo dotazovat. Požadovaná oprávnění přiřazená k danému ID uživatele (`VMCUser`) zajistí, že klient může spustit operace na virtuálním počítači a v prostředí VMware. Toto ID uživatele musí mít oprávnění VMware, která jsou popsaná ve výše uvedené technické poznámce.

Chcete-li vytvořit roli serveru vCenter pro operace zálohy a obnovy, použijte funkci klienta VMware vSphere **Přidat roli**. Musíte vybrat volbu `Šířit na podřízené položky`, přidáváte-li oprávnění pro toto ID uživatele (`VMCUser`). Kromě toho zvažte přidání dalších oprávnění k této roli pro ostatní úlohy kromě zálohy a obnovy. Pro volbu `VMCUser` je vynucení objekt nejvyšší úrovně.

Oprávnění serveru vCenter požadovaná k ochraně datových středisek VMware s pohledem modulu IBM Spectrum Protect vSphere Client plug-in pro grafické rozhraní produktu Data Protection for VMware vSphere

Modul IBM Spectrum Protect vSphere Client plug-in vyžaduje sadu oprávnění, která jsou oddělená od oprávnění vyžadovaných pro přihlášení ke grafickému rozhraní.

Během instalace jsou vytvořena následující vlastní oprávnění pro modul IBM Spectrum Protect vSphere Client plug-in:

- **Datové středisko** > **IBM Data Protection**
- **Globální** > **Konfigurovat produkt IBM Data Protection**

Vlastní oprávnění, která jsou požadována pro modul IBM Spectrum Protect vSphere Client plug-in, jsou registrována jako oddělené rozšíření. Klíč rozšíření oprávnění je `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Tato oprávnění umožňují administrátorovi VMware povolit a zakázat přístup k obsahu modulu IBM Spectrum Protect vSphere Client plug-in. Pouze uživatelé s těmito vlastními oprávnění na požadovaném objektu VMware mohou získat přístup k obsahu modulu IBM Spectrum Protect vSphere Client plug-in. Jeden modul IBM Spectrum Protect vSphere Client plug-in je registrován pro každý server a je sdílen všemi hostiteli grafického rozhraní, kteří jsou konfigurováni pro podporu serveru vCenter.

Z webového klienta VMware vSphere musíte vytvořit roli pro uživatele, kteří mohou provádět funkce ochrany dat pro virtuální počítače pomocí modulu IBM Spectrum Protect vSphere Client plug-in. Pro tuto roli, kromě standardních oprávnění role administrátora virtuálního počítače požadovaných webovým klientem, musíte uvést oprávnění **Datové středisko** > **IBM Data Protection**. Pro každé datové středisko přiřaďte tuto roli pro každého uživatele nebo skupinu, kde chcete udělit oprávnění, aby uživatel mohl spravovat virtuální počítače.

Oprávnění **Globální** > **IBM Data Protection** je vyžadováno pro uživatele na úrovni produktu vCenter. Toto oprávnění umožňuje uživateli spravovat, upravit nebo vymazat připojení mezi serverem vCenter a webovým serverem grafického rozhraní produktu Data Protection for VMware vSphere. Přiřaďte toto oprávnění k administrátorům, kteří jsou obeznámeni s grafickým rozhraním produktu Data Protection for VMware vSphere chránícím jejich příslušné servery vCenter. Svoje připojení k modulu IBM Spectrum Protect vSphere Client plug-in spravujte na stránce rozšíření **Připojení**.

Následující příklad zobrazuje, jak řídit přístup k datovým střediskům pro dvě skupiny uživatelů. Skupina 1 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska `NewYork DC` a `Boston_DC`. Skupina 2 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska `LosAngeles_DC` a `SanFranciso_DC`.

Z klienta VMware vSphere vytvořte například roli "IBMDataProtectManage", přiřaďte standardní oprávnění role administrátora virtuálních počítačů a také oprávnění **Datové středisko** > **IBM Data Protection**.

Pro skupinu 1 přiřaďte roli "IBMDataProtectManage" k datovým střediskům `NewYork DC` a `Boston_DC`. Pro skupinu 2 přiřaďte roli "IBMDataProtectManage" k datovým střediskům `LosAngeles_DC` a `SanFranciso_DC`.

Uživatelé v každé skupině mohou používat modul IBM Spectrum Protect vSphere Client plug-in v prostředí webového klienta vSphere ke správě virtuálních počítačů pouze ve svých odpovídajících datových střediscích.

Problémy týkající se nedostatečných oprávnění

Když nemá uživatel webového prohlížeče dostatečná oprávnění k jakémukoli datovému středisku, přístup k pohledu je blokován. Namísto toho se objeví chybová zpráva GVM2013E, která oznamuje, že uživatel není autorizován pro přístup k žádným spravovaným datovým střediskům vzhledem k nedostatečným oprávněním. Jsou rovněž k dispozici další nové zprávy, které informují uživatele o problémech způsobených nedostatečnými oprávněními. Chcete-li vyřešit případné problémy související s oprávněními, ujistěte se, že role uživatele je nastavena tak, jak je popsáno v předchozích sekcích. Role uživatele musí mít všechna oprávnění, která jsou identifikována v tabulce Požadovaných oprávnění ID uživatele serveru vCenter a modulu pro přesouvání dat, a tato oprávnění musí být použita na úrovni datového centra se zaškrtávacím políčkem `Šířit na podřízené prvky`.

Když nemá uživatel modulu IBM Spectrum Protect vSphere Client plug-in dostatečná oprávnění pro datové středisko, funkce ochrany dat pro toto datové středisko a jeho obsah nejsou v rozšíření k dispozici.

Když ID uživatele IBM Spectrum Protect (uvedené volbou `VMCUser`) obsahuje nedostatečná oprávnění pro operace zálohy a obnovy, zobrazí se následující zpráva:

```
ANS9365E Chyba rozhraní API VMware vStorage.
"Oprávnění pro provedení této operace bylo odepřeno."
```

Když ID uživatele IBM Spectrum Protect obsahuje nedostatečná oprávnění pro zobrazení počítače, zobrazí se následující zpráva:

```
Příkaz Backup VM byl spuštěný.
Celkový počet virtuálních počítačů ke zpracování: 1
ANS4155E Virtuální počítač 'tango' nebyl na serveru VMware nalezen.
ANS4148E Úplná záloha virtuálního počítače 'foxtrot' selhala s návratovým kódem 4390
```

Další informace k používání oprávnění najdete v poznámce **Oprávnění serveru vCenter požadovaná pro použití modulu pro přesouvání dat**.

Chcete-li načíst informace o protokolu prostřednictvím serveru VMware Virtual Center a hledat problémy s oprávněním, postupujte takto:

1. V nabídce **Nastavení serveru vCenter** vyberte volbu **Volby protokolování** a nastavte volbu "**Protokolování vCenter** na hodnotu **Trivia (Trivia)**.
2. Znovu vyvolejte chybu oprávnění.
3. Resetujte volbu **Protokolování vCenter** na předchozí hodnotu, což zabraňuje záznamu nadměrného množství informací v protokolu.
4. V nabídce **Systémové protokoly** vyhledejte nejaktuálnější protokol serveru vCenter (`vpxd-wxyz.log`) a vyhledejte řetězec `NoPermission`. Například:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Tato zpráva protokolu označuje, že ID uživatele neobsahovalo dostatečná oprávnění pro vytvoření snímku (`createSnapshot`).

Instalace komponent produktu Data Protection for VMware

Můžete nainstalovat všechny komponenty nebo jen některé z nich, které jsou dostupné v balíku Data Protection for VMware pro váš operační systém.

Informace o této úloze

Pomocí instalačního programu Data Protection for VMware můžete nainstalovat následující komponenty:

- IBM Spectrum Protectzotavení
- Windows Rozhraní příkazového řádku agenta zotavení
- Windows Dokumentace (soubor Readme a soubor s upozorněním)
- Soubor zpřístupnění Data Protection for VMware
- Data Protection for VMware vSphere
- Funkce modulu pro přesouvání dat, což také zahrnuje tyto položky:
  - grafické uživatelské rozhraní modulu pro přesouvání dat
  - webový klient modulu pro přesouvání dat
  - běhové soubory rozhraní API klienta (64bitové)
  - příkazový řádek administrativního klienta
  - běhové soubory rozhraní API produktu VMware vStorage

Můžete zvolit úplnou instalaci, nebo použít volbu Rozšířená instalace, chcete-li nainstalovat modul pro přesouvání dat (server proxy pro připojení), agenta zotavení a požadované balíky podpory.

Tip: Můžete vytvořit několik modulů pro přesouvání dat na stejném systému, jako je software Data Protection for VMware nebo můžete vytvořit moduly pro přesouvání dat na vzdálených systémech. Tato konfigurace navyšuje prostředky dostupné pro použití v produktu Data Protection for VMware. Systémy s nainstalovaným modulem pro přesouvání dat se nazývají záložní servery vStorage.

Získání instalačního balíku produktu Data Protection for VMware

Můžete získat instalační balík produktu Data Protection for VMware ze stránky se soubory ke stažení IBM, jako například IBM Passport Advantage.

Než začnete

Linux

Pokud plánujete stažení souborů, nastavte omezení uživatelů systému pro maximální velikost souboru na neomezenou, čímž zajistíte, že se soubory stáhnou správně:

1. Chcete-li se dotázat na hodnotu maximální velikost souboru, zadejte následující příkaz:

```
ulimit -Hf
```

2. Pokud není omezení uživatelů systému pro maximální velikost souboru nastaveno na neomezeno, změníte jej na neomezeno, pokud budete postupovat podle pokynů v dokumentaci pro svůj operační systém.

Postup

1. Stáhněte odpovídající soubor balíku z některého z níže uvedených webů:
   - Pro první instalaci nebo nové vydání přejděte do sekce Passport Advantage na adrese: http://www.ibm.com/software/lotus/passportadvantage/. Passport Advantage je jediný web, odkud můžete stáhnout licencovaný soubor balíku.
   - Nejnovější informace, aktualizace a opravy údržby viz web podpory produktu IBM Spectrum Protect: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.
2. Pokud jste stáhli balík ze stránky stahování IBM, postupujte takto:
   a. Stáhněte soubor balíku do adresáře podle vlastní volby. Cesta smí obsahovat maximálně 40 znaků. Ujistěte se, že instalační soubory extrahujete do prázdného adresáře. Neextrahujte do adresáře, který obsahuje dříve extrahované soubory ani žádné jiné soubory.
   b. Linux Ujistěte se, že oprávnění spustitelného souboru je nastaveno pro balík. Je-li to nezbytné, změňte oprávnění k souboru zadáním následujícího příkazu:
      ```
      chmod a+x název_balíku.bin
      ```
   c. Linux Extrahujte balík zadáním následujícího příkazu:
      ```
      ./název_balíku.bin
      ```
      kde *název_balíku* označuje název staženého souboru.
   d. Windows Extrahujte balík poklepáním na *název_balíku*, kde *název_balíku* je název staženého souboru.

Instalace komponent produktu Data Protection for VMware pomocí průvodce instalací

Pomocí průvodce instalací můžete nainstalovat komponenty produktu Data Protection for VMware.

Informace o této úloze

Windows Pomocí instalačního programu sady můžete nainstalovat produkt Data Protection for VMware i modul pro přesouvání dat.

Linux K instalaci produktu Data Protection for VMware a modulu pro přesouvání dat můžete použít samostatný instalační program.

Instalace komponent Data Protection for VMware na systémech Windows

Pomocí průvodce instalací nainstalujte komponenty Data Protection for VMware a funkce.

Než začnete

Před instalací komponent Data Protection for VMware se ujistěte, že splňujete následující požadavky:

- ID uživatele s oprávněním administrátora k přístupu.
- Síťová konektivita k serveru VMware vCenter Server 6.x (nebo novější) s oprávněním přístupu administrátora.
- Síťová konektivita k serveru IBM Spectrum Protect s přístupem administrátora (oprávnění **Systém** nebo **Neomezená doména zásad**). Tento server musí být dostupný a spuštěn.
- Ujistěte se, že jste přezkoumali následující požadavky:
  - “Systémové požadavky” na stránce 11

- “Požadované oprávnění k instalaci” na stránce 14
- “Požadované komunikační porty” na stránce 15

Než nainstalujete produkt Data Protection for VMware, musíte být obeznámeni s následujícími volbami:

Typ instalace

Typická instalace
U typických instalací jsou nainstalovány všechny komponenty a funkce produktu Data Protection for VMware.

Rozšířená instalace
Panel Rozšířená instalace poskytuje volbu instalace individuálního modulu pro přesouvání dat. Proces nainstaluje modul pro přesouvání dat (server proxy pro připojení), agenta zotavení a požadované balíky podpory na systému. Pomocí této volby instalace přidejte individuální moduly pro přesouvání dat. Tato volba také nainstaluje agenty ochrany aplikací, aby se umožnilo zotavení individuálních databází. Po instalaci můžete použít grafické rozhraní produktu IBM Spectrum Protect GUI ke konfiguraci modulu pro přesouvání dat a služeb prostřednictvím modulu plug-in VMware vSphere.

Informace o této úloze

Pomocí instalačního programu sady můžete nainstalovat produkt Data Protection for VMware. Soubor `spinstall.exe` pro instalační program sady je umístěn v kořenovém adresáři instalačního balíku.

Chcete-li získat seznam komponent a funkcí, které můžete nainstalovat, prohlédněte si sekci “Instalovatelné komponenty” na stránce 1.

Postup

Chcete-li nainstalovat produkt Data Protection for VMware, proveďte postup uvedený v umístění souboru `spinstall.exe` pro komponentu, kterou jste se rozhodli nainstalovat:

1. Poklepejte na soubor `spinstall.exe`.
2. Postupujte podle pokynů průvodce instalací zvolených komponent.

Jak pokračovat dále

Chcete-li získat přístup ke grafickému rozhraní produktu Data Protection for VMware vSphere, postupujte takto:

- “Přístup do grafického rozhraní produktu Data Protection for VMware vSphere” na stránce 27

Průvodce konfigurací se automaticky zobrazí při prvním spuštění grafického rozhraní.

Instalace produktu Data Protection for VMware v systémech Linux
Instalace produktu Data Protection for VMware na systémech Linux pomocí režimu InstallAnywhere.

Než začnete

Před instalací produktu Data Protection for VMware se ujistěte, že splňujete následující požadavky:

- Ujistěte se, než budete pokračovat, že ID uživatele má požadovanou úroveň oprávnění a že jsou požadované komunikační porty otevřené.
- Instalační proces vytvoří uživatele `tdpvmware`. Všechny příkazy **`vmcli`** musíte zadat jako uživatel `tdpvmware` ID uživatele root.
- Pokud provádíte instalace v režimu konzoly, je vyžadován server X Window.
- Ujistěte se, že jste přezkoumali následující požadavky:
  - “Systémové požadavky” na stránce 11
  - “Požadované oprávnění k instalaci” na stránce 14
  - “Požadované komunikační porty” na stránce 15

Postup

Chcete-li instalovat produkt Data Protection for VMware, postupujte takto:

1. Z kořenového adresáře instalační složky přejděte do adresáře `CD/Linux/DataProtectionForVMware`.
2. V příkazovém řádku zadejte tento příkaz:

```
./install-Linux.bin
```

Výsledky

Pokud obdržíte jakákoli varování nebo chyby, zkontrolujte soubory protokolu, abyste získali další informace. Viz “Aktivita souboru protokolu” na stránce 78.

Pokud jste kvůli selhání nebyli schopni nainstalovat produkt Data Protection for VMware, prohlédněte si proceduru "Ruční odebrání produktu Data Protection for VMware" v sekci “Odinstalace produktu Data Protection for VMware na systému Linux” na stránce 34.

Provedení čisté instalace produktu Data Protection for VMware na systému Linux

Pokud je instalace na systému Linux přerušena, můžete ji obvykle restartovat. Avšak pokud restartování instalace selže, požaduje se čistá instalace.

Informace o této úloze

Před spuštěním čisté instalace se ujistěte, že produkt je odebrán. Chcete-li zajistit čisté prostředí, postupujte takto:

Postup

1. Pokud je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere, postupujte takto:
   a) Zadáním následujícího příkazu zastavte komponentu rozhraní příkazového řádku produktu Data Protection for VMware:
   `/etc/init.d/vmcli stop`
   b) Zadáním následujícího příkazu zastavíte webový server grafických rozhraní produktu Data Protection for VMware:
   `/etc/init.d/webserver stop`
   c) Zadáním následujícího příkazu odeberte balík `.rpm`:
   `rpm -e TIVsm-TDPVMwarePlugin`
2. Odeberte položky produktu Deployment Engine:
   a) Chcete-li vypsat všechny položky produktu Deployment Engine, zadejte následující příkaz:
   `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b) Chcete-li odebrat všechny položky produktu Deployment Engine, zadejte následující příkaz:
   `/usr/ibm/common/acsi/bin/deleteRootIU.sh` *<UUID> <diskriminant>*
   c) Odeberte adresář `/var/ibm/common`.
   d) Odeberte adresář `/usr/ibm/common`.
   e) Vyčistěte adresář `/tmp` odebráním souboru `acu_de.log`, pokud existuje.
   f) Odeberte adresář `/tmp` obsahující ID uživatele instalovaného v produktu Deployment Engine.
   g) Odeberte všechny položky produktu Deployment Engine ze systémového souboru `/etc/inittab`. Položky jsou odděleny pomocí oddělovačů `#Begin AC Solution Install block` a `#End AC Solution Install block`. Odeberte všechen text mezi těmito oddělovači a odeberte vlastní oddělující text.
   h) Odeberte odkazy produktu Deployment Engine ze systémového souboru `/etc/services`.
3. Odeberte všechny soubory produktu Data Protection for VMware z neúspěšné instalace:

a) Odeberte soubory v adresáři <*USER_INSTALL_DIR*>, který je cestou, ve které byl učiněn pokus o neúspěšnou instalaci. Například: `/opt/tivoli/tsm/TDPVMware/`

b) Odeberte všechny zástupce na pracovní ploše.

4. Zazálohujte globální soubor registru (`/var/.com.zerog.registry.xml`). Po zálohování tohoto souboru odeberte všechny značky odkazující produkt Data Protection for VMware.
5. Odeberte soubory protokolu pod kořenem, které obsahují řetězec `TDPVMware`.
   Například:
   `IA-TDPVMware-00.log` nebo `IA-TDPVMware_Uninstall-00.log`.
6. Odeberte uživatele, který spustil rozhraní příkazového řádku produktu Data Protection for VMware.
   a) Vydejte následující příkazy:

```
userdel -r tdpvmware
```

   b) Vydejte následující příkazy:

```
groupdel tdpvmware
```

   Tip: V některých verzích systému Linux příkaz **userdel** také odebere skupinu, pokud neexistují žádní další přidružení uživatelé. Jako výsledek, ignorujte všechny zprávy o selhání související s příkazem.

Výsledky
Po dokončení těchto kroků spusťte čistou instalaci.

Instalace komponent produktu Data Protection for VMware v bezobslužném režimu

Produkt Data Protection for VMware můžete nainstalovat na pozadí. Během bezobslužné instalace ne nezobrazí žádné zprávy.

Informace o této úloze

Windows Pomocí instalačního programu sady můžete nainstalovat produkt Data Protection for VMware i modul pro přesouvání dat.

Linux K instalaci produktu Data Protection for VMware a modulu pro přesouvání dat můžete použít samostatný instalační program.

Bezobslužná instalace produktu Data Protection for VMware na systémy Windows

Instalujte všechny komponenty produktu Data Protection for VMware a funkce modulu pro přesouvání dat pomocí instalačního programu sady v bezobslužném režimu.

Než začnete

Před instalací produktu Data Protection for VMware a funkce modulu pro přesouvání dat se ujistěte, že váš systém splňuje požadavky v těchto sekcích:

- “Systémové požadavky” na stránce 11
- “Požadované oprávnění k instalaci” na stránce 14
- “Požadované komunikační porty” na stránce 15

Informace o této úloze

Omezení: Na systému Windows jsou některá umístění instalací pevná. Chcete-li vyhledat instalační adresáře komponent, prohlédněte si téma “Instalovatelné komponenty” na stránce 1.

Postup

Chcete-li instalovat produkt Data Protection for VMware, postupujte takto:

1. Z příkazového řádku zadejte tento příkaz:

```
cd extrahovaná_složka\TSMVMWARE_WIN
```

2. Zadejte tento příkaz:

```
spinstall.exe /silent
```

Následující zpráva se zobrazí při prvním připojení svazku:

```
Ovladač virtuálního svazku ještě není registrován. Agent zotavení může registrovat
ovladač nyní. Během registrace se může zobrazit varování s logem
systému Microsoft Windows.
Chcete-li umožnit dokončení této registrace, přijměte varování.
Chcete registrovat ovladač virtuálního svazku nyní?
```

Chcete-li pokračovat, zadejte **Ano**, aby se zaregistroval ovladač virtuálního svazku.

Související úlohy

"Odinstalace produktu Data Protection for VMware pro systém Windows v bezobslužném režimu" na stránce 33
Můžete bezobslužně odinstalovat produkt Data Protection for VMware na operačním systému Windows.

Instalace systémů Data Protection for VMware on Linux v bezobslužném režimu

Můžete přizpůsobit, které funkce produktu Data Protection for VMware se mají na operačním systému Linux bezobslužně instalovat.

Než začnete

Před instalací produktu Data Protection for VMware se ujistěte, že splňujete následující požadavky:

- Ujistěte se, než budete pokračovat, že ID uživatele má požadovanou úroveň oprávnění a že jsou požadované komunikační porty otevřené.
- Instalační proces vytvoří uživatele `tdpvmware`. Všechny příkazy **`vmcli`** musíte zadat jako uživatel `tdpvmware` ID uživatele root.
- Pokud provádíte instalace v režimu konzoly, je vyžadován server X Window.
- Ujistěte se, že jste přezkoumali následující požadavky:
  - "Systémové požadavky" na stránce 11
  - "Požadované oprávnění k instalaci" na stránce 14
  - "Požadované komunikační porty" na stránce 15

Informace o této úloze

Omezení: Na systému Linux jsou všechna umístění instalace pevná. Chcete-li vyhledat instalační adresáře komponent, prohlédněte si téma "Instalovatelné komponenty" na stránce 1.

Produkt Data Protection for VMware poskytuje následující funkce bezobslužné instalace pro operační systémy Linux:

Tabulka 7. Funkce bezobslužné instalace produktu Data Protection for VMware

Funkce	Popis	Instalovaná standardně?
Docs	Soubor Readme	Ano

Tabulka 7. Funkce bezobslužné instalace produktu Data Protection for VMware (pokračování)		
Funkce	**Popis**	**Instalovaná standardně?**
TDPVMwareDM	Instalace této funkce zahrnuje soubor zpřístupnění. Umožňuje produktu IBM Spectrum Protect spustit následující typy zálohy: • Periodická přírůstková záloha virtuálního počítače • Úplná přírůstková trvalá záloha virtuálního počítače • Přírůstková trvalá přírůstková záloha virtuálního počítače Pokud odlehčíte pracovní zátěže zálohy, musí být tento soubor instalován na záložním serveru vStorage.	Ano
TDPVMwareGUI	Data Protection for VMware vSphere. **Poznámka:** Také zahrnuje instalaci souboru zpřístupnění.	Ne

Postup

Chcete-li nainstalovat produkt Data Protection for VMware, v adresáři, kam jste extrahovali instalační balík, postupujte takto:

1. Otevřete soubor *cesta*`../Linux/DataProtectionForVMware/installer.properties` a zrušte komentář u následující položky, čímž přijmete licenci (kde *cesta* je instalační složka):

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. Vyberte si jednu z následujících metod pro instalaci komponent Data Protection for VMware:
   - Pro vlastní instalaci otevřete složku `CD/Linux/DataProtectionForVMware` a zadejte následující příkaz:

     ```
     ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
     ```

   - Pro vlastní instalaci postupujte takto:
     a. Upravte soubor `installer.properties` pomocí odpovídajících hodnot:
        1) Uveďte **`INSTALL_MODE=Custom`**. Ujistěte se, že je z tohoto příkazu odebrán znak křížku (#).
        2) Pomocí volby **`CHOSEN_INSTALL_FEATURE_LIST`** uveďte funkce, které se mají instalovat. Pomocí této volby jsou například instalovány všechny funkce:

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

     b. Ze složky `CD/Linux/DataProtectionForVMware` zadejte následující příkaz:

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

První kroky po instalaci produktu Data Protection for VMware

Po instalaci produktu Data Protection for VMware se připravte na konfiguraci. Použití průvodce konfigurací je upřednostňovanou metodou konfigurace produktu Data Protection for VMware.

Pracovní list konfigurace

Pomocí tohoto pracovního listu zaznamenáte informace, které potřebujete, budete-li konfigurovat a spravovat produkty Data Protection for VMware. Pracovní list by vám měl pomoci zapamatovat si hodnoty, které jste uvedli po konfiguraci.

Tabulka 8. Pracovní list konfigurace produktu Data Protection for VMware

Položka	Vaše hodnota	Poznámky
Informace o serveru IBM Spectrum Protect		
IBM Spectrum Protect adresa serveru		
IBM Spectrum Protect port serveru		
ID/heslo administrátora serveru IBM Spectrum Protect		
Port administrátora serveru IBM Spectrum Protect		
Volby definice uzlu		
Předpona, která se přidá k uzlům		
Doména zásady, která se použije při registraci nových uzlů		
Název uzlu/heslo vCenter		
Název uzlu/heslo VMCLI		
Názvy/hesla uzlu datového střediska **Zapamatujte si:** Můžete vytvořit více uzlů datového střediska.		Název uzlu datového střediska se skládá z uvedené předpony, následované znakem podtržení, dále následované názvem datového střediska. Například: *nodePrefix_datacenterName*
Názvy/hesla uzlu modulu pro přesouvání dat na záložním serveru vStorage **Zapamatujte si:** Můžete vytvořit více uzlů modulu pro přesouvání dat.		Uzel modulu pro přesouvání dat se skládá z názvu uzlu datového střediska, následovaného znakem podtržení, následovaného hodnotou DM. Například: *datacenterNodename*_DM
Názvy/hesla uzlů modulu pro přesouvání dat na vzdálených serverech **Zapamatujte si:** Můžete vytvořit více uzlů modulu pro přesouvání dat, které nejsou na záložním serveru vStorage.		
Uzel serveru proxy připojení Uzel serveru proxy připojení se používá k obnovení dat.	Windows: Linux:	

Přístup do grafického rozhraní produktu Data Protection for VMware vSphere

Pomocí grafického rozhraní produktu Data Protection for VMware vSphere zazálohujete, obnovíte a můžete spravovat virtuální počítače v prostředí VMware vCenter.

Než začnete

Než budete moci získat přístup ke grafickému rozhraní produktu Data Protection for VMware vSphere, musíte během instalace zvolit volbu k ochraně dat v prostředí vSphere.

Procedura

- Pokud jste během instalace vybrali volbu **Povolit přístup ke grafickému rozhraní pomocí webového prohlížeče**, můžete do grafického rozhraní produktu Data Protection for VMware vSphere získat přístup z prohlížeče:
  1. Otevřete webový prohlížeč a zadejte následující adresu URL:

     ```
     https://název_hostitele:port/TsmVMwareUI
     ```

     kde:

     – *název_hostitele* je název systému, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere
     – *port* je číslo portu, na kterém je k přístupné grafické rozhraní vSphere. Výchozí číslo portu je 9080. Pro zabezpečené porty je výchozí hodnota 9081.
  2. Přihlaste se pomocí svého ID uživatele a hesla prostředí vCenter.
- Pokud jste nevybrali během instalace volbu **Povolit přístup ke grafickému rozhraní pomocí webového prohlížeče**, můžete grafické rozhraní produktu Data Protection for VMware vSphere spustit tímto postupem:
  1. Otevřete klienta VMware vSphere Client a přihlaste se pomocí ID uživatele a hesla vCenter.
  2. V panelu **Řešení a aplikace** klienta vSphere klepněte na ikonu grafického rozhraní produktu Data Protection for VMware vSphere.

Upgrade produktu Data Protection for VMware

Produkt Data Protection for VMware můžete upgradovat z předchozí verze softwaru.

Informace o kompatibilitě se staršími verzemi viz technická poznámka 1993819.

Upgrade z verze 7.1.8: Jestliže se během procesu upgradu objeví zpráva s dotazem, zda chcete přepsat existující soubor `jextract`, vyberte volbu **Ano pro všechny**.

Upgrade produktu Data Protection for VMware

Tato procedura dokumentuje, jak upgradovat na produkt Data Protection for VMware V8.1.10.

Než začnete

Důležité: Tato procedura upgradu se používá pro systém, který nemá nainstalován produkt IBM Spectrum Protect Snapshot for VMware.

Musíte mít oprávnění administrátora, chcete-li upgradovat produkt Data Protection for VMware.

Aktualizace v existujícím grafickém rozhraní produktu Data Protection for VMware vSphere jsou zpracovány následujícím způsobem:

- Soubory s parametry jsou zálohovány před začátkem procesu upgradu grafického rozhraní produktu Data Protection for VMware vSphere.
- Použijí se stejná čísla portu databáze Derby a výchozího základního portu aplikačního serveru WebSphere Application Server.
- Linux Hodnoty v profilu (`vmcliprofile`) jsou použity pro komponentu rozhraní příkazového řádku produktu Data Protection for VMware.

Omezení:

- Windows Když byl produkt IBM Spectrum Protect for Virtual Environments nainstalován do jiného než výchozího umístění, proces upgradu nainstaluje funkce produktu IBM Spectrum Protect for Virtual Environments V8.1.10 do výchozího instalačního adresáře. Nemůžete provést upgrade do jiného než výchozího umístění. Prohlédněte si dílčí témata v sekci “Instalovatelné komponenty” na stránce 1, kde najdete výchozí instalační adresáře pro každou funkci.

- Windows | Linux Přechod na vyšší verzi nemůže instalovat nové komponenty.

  Pokud má například vaše předchozí verze instalováno pouze grafické rozhraní agenta zotavení, neinstaluje proces upgradu rozhraní příkazového řádku agenta zotavení. V takovém scénáři musíte spustit instalační program znovu a pak vybrat chybějící komponentu pro instalaci.
- Windows | Linux Služba vCenter vyžaduje přístup k názvu domény hostitele grafického uživatelského rozhraní.

  Název domény hostitele grafického uživatelského rozhraní použité v upgradu musí být dosažitelné službou vCenter, aby bylo možné upgradovat modul plug-in Data Protection vSphere. Není-li název domény dosažitelný, pak bude nutné po upgradu znovu registrovat modul plug-in.
- Linux Verze agenta zotavení na systému Linux musí být stejná jako verze agenta zotavení na zástupci systému Windows. Proto, pokud provádíte upgrade agenta zotavení na systému Linux, musíte také upgradovat verzi agenta zotavení na zástupci systému Windows.

Postup

Chcete-li upgradovat produkt Data Protection for VMware, postupujte takto:

1. Zastavte všechny komponenty a služby produktu Data Protection for VMware, které jsou spuštěné.
2. Uvolněte všechny připojené virtuální svazky.

   Pro uvolnění svazků můžete použít grafické rozhraní nebo rozhraní příkazového řádku agenta zotavení (příkaz **`mount del`**).
3. Postupujte podle pokynů v tématu “Instalace komponent Data Protection for VMware na systémech Windows” na stránce 21.

   Poznámka: Linux Pokud je nainstalován modul pro přesouvání dat verze V6.x, musíte jej odinstalovat, než nainstalujete produkt V8.1.10. Postupujte podle pokynů v tématu Odinstalace klienta IBM Spectrum Protect Linux x86_64.
4. Stáhněte balík kódu.
5. Ve složce, kam jste uložili balík kódu, spusťte proces upgradu:

   a) Windows
   Spusťte soubor `spinstall.exe`.

   b) Linux
   Spusťte soubor `install-Linux.bin`.

   Na počítači můžete nainstalovat pouze jedno grafické rozhraní produktu Data Protection for VMware vSphere. Jako výsledek není na stejném počítači povoleno více grafických rozhraní produktu Data Protection for VMware vSphere.

Upgrade produktu Data Protection for VMware na 64bitovém systému Windows v bezobslužném režimu

Produkt Data Protection for VMware můžete bezobslužně upgradovat na podporovaném 64bitovém operačním systému.

Než začnete

Když byla nainstalována verze produktu Data Protection for VMware V6.x do jiného než výchozího umístění, proces bezobslužného upgradu nainstaluje funkce produktu Data Protection for VMware V8.1.10 do výchozího instalačního adresáře. Nemůžete provádět bezobslužný upgrade do jiného než výchozího umístění. Prohlédněte si dílčí témata v sekci “Instalovatelné komponenty” na stránce 1, kde najdete výchozí instalační adresáře pro každou funkci.

Postup

Chcete-li upgradovat produkt Data Protection for VMware, postupujte takto:

1. Zastavte všechny spuštěné komponenty Data Protection for VMware.

2. Uvolněte všechny připojené virtuální svazky.

   Pro uvolnění svazků můžete použít grafické rozhraní nebo rozhraní příkazového řádku agenta zotavení (příkaz **mount del**).
3. Uvolněte všechny připojené virtuální svazky.

   Pro uvolnění svazků můžete použít grafické rozhraní nebo rozhraní příkazového řádku agenta zotavení (příkaz **mount del**).
4. Stáhněte balík kódu.
5. Přejděte do složky produktu Data Protection for VMware.
6. V okně příkazového řádku zadejte tento příkaz:

   ```
   spinstall.exe /silent REGISTER_EXTENSION=1 VCENTER_HOSTNAME=<hostname>
   VCENTER_USERNAME=<username> VCENTER_PASSWORD=<pass> /debuglog<file_path>
   ```

Upgrade produktu Data Protection for VMware na systému Linux v bezobslužném režimu

Produkt Data Protection for VMware můžete upgradovat na podporovaném operačním systému Linux.

Informace o této úloze

Použijte následující parametry Data Protection for VMware s funkcí bezobslužné instalace:

Tabulka 9. Parametry aktualizace bezobslužné instalace produktu Data Protection for VMware

Parametr	Popis	Výchozí hodnota
VCENTER_HOSTNAME	Úplný název domény nebo adresa IP serveru vCenter.	Žádný
VCENTER_USERNAME	ID uživatele vCenter. Toto ID uživatele musí být administrátorem VMware, který má oprávnění registrovat a rušit registraci rozšíření.	Žádný
VCENTER_PASSWORD	Heslo vCenter.	Žádný
DIRECT_START	Chcete-li získat přístup do grafického rozhraní produktu Data Protection for VMware vSphere ve webovém prohlížeči, uveďte **DIRECT_START=YES**. Do grafického rozhraní produktu Data Protection for VMware vSphere lze přistupovat prostřednictvím záložky adresy URL na webový server grafického rozhraní. Pokud nechcete přistupovat do grafického rozhraní produktu Data Protection for VMware vSphere ve webovém prohlížeči, uveďte **DIRECT_START=NO**.	ANO **Důležité:** Po dokončení upgradu již nelze změnit hodnotu **DIRECT_START**, pouze při přeinstalaci produktu.

Postup

Chcete-li upgradovat produkt Data Protection for VMware, postupujte takto:

1. Ujistěte se, že neexistují žádné aktivní relace zálohování, obnovy nebo připojení.
2. Ujistěte se, že jsou zavřena všechna grafická rozhraní produktu Data Protection for VMware vSphere nebo grafická rozhraní agenta zotavení.
3. Stáhněte balík kódu.
4. Ze složky Data Protection for VMware přejděte do složky Linux.
5. V okně příkazového řádku zadejte příkaz `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` s upřednostňovanými parametry.
   Například: `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true -DVCENTER_HOSTNAME=9.11.90.86 -DVCENTER_USERNAME=administrator@vsphere.local -DVCENTER_PASSWORD=**** -DREGISTER_EXTENSION=yes -DDIRECT_START=yes`

Upgrade produktu Data Protection for VMware v prostředí s propojeným režimem serveru vCenter

Všichni hostitelé grafického rozhraní produktu Data Protection for VMware musí být aktualizováni včas, aby povolili komponenty produktu Data Protection for VMware za účelem podpory aktuálních funkcí propojeného režimu VMware.

Informace o této úloze

Poznámka: Tyto informace jsou specifické pro verze 6.0, 6.5 & 6.7 aplikace vSphere spuštěné na serveru VMware vCenter.

Propojený režim serveru VMware vCenter je nástroj, který poskytuje přehled zón správy, aby servery mohly podporovat větší počty virtuálních počítačů. Modul plug-in produktu IBM Spectrum Protect Data Protection for VMware je kompatibilní s prostředím VMware spuštěným v propojeném režimu. Další informace o této funkci VMware naleznete v dokumentaci VMware na webu Rozšířený propojený režim vCenter.

Když jsou servery vCenter v propojeném režimu, existuje jediný pohled na všechny servery vCenter přes uživatelské rozhraní vSphere. Stejné uživatelské rozhraní je viditelné při přihlášení na jakýkoli ze serverů vCenter, které jsou propojené. V důsledku toho se modul plug-in produktu IBM Spectrum Protect Data Protection zobrazí na všech serverech vCenter, i když byl nainstalován a nakonfigurován pouze na jediném serveru vCenter.

Zatímco je modul plug-in viditelný na každém serveru vCenter, funkčnost modulu plug-in je k dispozici pouze na tom serveru vCenter, který má přidruženého hostitele grafického rozhraní IBM Spectrum Protect Data Protection for VMware.

Při upgradu prostředí s propojeným režimem serveru vCenter vezměte v úvahu tyto záležitosti:

- Při použití serverů vCenter v propojeném režimu způsobí upgrade prvního serveru vCenter, že všechny propojené servery vCenter uvidí modul plug-in novější úrovně. Modul plug-in produktu IBM Spectrum Protect Data Protection for VMware byl vyvinut, aby byl kompatibilní s jedním hostitelem grafického rozhraní s vydáním nižší úrovně. Například modul plug-in Data Protection for VMware V8.1.6 je stále kompatibilní s hostitelem grafického rozhraní Data Protection for VMware V8.1.4.
- Zatímco hostitel grafického rozhraní nižší úrovně bude stále fungovat s novějším modulem plug-in, funkce zavedené v novější verzi nebudou fungovat. Musíte včas aktualizovat všechny hostitele grafického rozhraní, abyste povolili úplnou funkčnost novějšího modulu plug-in.

Příklad

Před upgradem na verzi 8.1.6 jsou servery vCenter1 a vCenter2 v propojeném režimu. Každý z nich má hostitele grafického rozhraní IBM Data Protection for VMware. Modul plug-in v rámci vSphere a hostitelé grafického rozhraní jsou ve verzi 8.1.4.

Server vCenter1 je nyní upgradován na verzi V8.1.6. Modul plug-in a hostitel1 grafického rozhraní jsou nyní na verzi 8.1.6. Uživatel, který se přihlásí k produktu vSphere serveru vCenter2, uvidí modul plug-in V8.1.6, ne modul plug-in V8.1.4. Uživatel pak může přejít na nabídku **IBM Spectrum Protect -> Konfigurovat -> Připojení** a uvidí, že vCenter1 má hostitele grafického rozhraní ve verzi 8.1.6, ale hostitel grafického rozhraní vCenter2 je stále na verzi 8.1.4.

Modul plug-in Spectrum Protect stále funguje pro prostředí vCenter2 stejným způsobem jako ve verzi 8.1.4. Rozdíl je, že všechny nové funkce pro verzi 8.1.6 nelze použít na serveru vCenter2, pouze vCenter1, dokud nebude dokončen upgrade V8.1.6 na hostitele grafického rozhraní serveru vCenter2.

Odinstalace produktu Data Protection for VMware

Proces odinstalace produktu Data Protection for VMware je stejný pro novou instalaci i pro upgradovanou verzi.

Odinstalace produktu Data Protection for VMware na systému Windows

Odinstalujte komponenty Data Protection for VMware a odeberte soubory a adresáře ze systému Windows.

Než začnete

Chcete-li zajistit úspěšnou odinstalaci, postupujte takto:

- Pokud další weboví hostitele grafického rozhraní produktu Data Protection for VMware používají modul IBM Spectrum Protect vSphere Client plug-in, neprovádějte zrušení registrace rozšíření webového klienta.

Informace o této úloze

Konfigurační soubory a soubory vlastností se po dokončení odinstalace nacházejí v adresáři `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config`.

Postup

1. Zastavte všechny spuštěné komponenty Data Protection for VMware.
2. Uvolněte všechny připojené virtuální svazky.
3. Odstraňte všechny existující zálohy virtuálního počítače pomocí příkazu `delete backup` modulu pro přesouvání dat.
4. Odeberte všechny nainstalované služby modulu pro přesouvání dat pomocí příkazu `dsmcutil remove`.

   Chcete-li získat seznam služeb, přejděte do adresáře `C:\Program Files\Tivoli\TSM\baclient \` a spusťte příkaz `dsmcutil list`.

   Odeberte služby pomocí příkazu, který se podobá následujícímu příkazu, přičemž upravte uvedený název pro vypsanou službu:

   ```
    dsmcutil remove /name:"TSM Remote Client Agent"
   dsmcutil remove /name:"TSM Client Acceptor"
   ```

5. Klepněte na nabídku **Start** > **Ovládací panel** > **Programy a funkce** > **Odinstalovat program**. Odinstalujte následující programy:
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware Suite
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware License
   - IBM Spectrum Protect JVM
6. Odeberte následující soubory a adresáře produktu Data Protection for VMware ze systému souborů, jsou-li přítomny.

   V případě produktu IBM Spectrum Protect for Virtual Environments 8.1.6 a novější odstraňte:

   ```
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   ```

   Můžete také odstranit:

   ```
   C:\Program Files\Tivoli\TSM
   ```

   pokud již nepotřebujete zbývající soubory protokolu a konfigurační soubory. Chcete-li si ponechat tyto soubory, jsou umístěny v adresáři `C:\Program Files\Tivoli\TSM\baclient`.

V případě produktu IBM Spectrum Protect for Virtual Environments 8.1.4 a starší odstraňte:

```
C:\IBM\tivoli
C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
C:\Program Files\Common Files\Tivoli
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
```

Můžete také odstranit:

```
C:\Program Files\Tivoli\TSM
```

pokud již nepotřebujete zbývající soubory protokolu a konfigurační soubory. Chcete-li si ponechat tyto soubory, jsou umístěny v adresáři `C:\Program Files\Tivoli\TSM\baclient`.

Jak pokračovat dále

Zkontrolujte, zda všechny komponenty byly odebrány ze systému.

Odinstalace produktu Data Protection for VMware pro systém Windows v bezobslužném režimu

Můžete bezobslužně odinstalovat produkt Data Protection for VMware na operačním systému Windows.

Informace o této úloze

Konfigurační soubory a soubory vlastností se po dokončení odinstalace nacházejí v adresáři `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config`.

Postup

Chcete-li odinstalovat produkt Data Protection for VMware, postupujte takto:

1. Zastavte všechny spuštěné komponenty Data Protection for VMware.
2. Uvolněte všechny připojené virtuální svazky.

   Pro uvolnění svazků můžete použít grafické rozhraní nebo rozhraní příkazového řádku agenta zotavení (příkaz **`mount del`**).
3. V okně příkazového řádku:
   - Zrušte registraci modulu plug-in Grafické rozhraní produktu Data Protection for VMware vSphere a odinstalujte komponentu Data Protection for VMware:
     a. Přejděte do následujícího adresáře v instalačním programu:

     ```
     TSMVMWARE_WIN\DPVMware
     ```

     b. Zadejte tento příkaz:

     ```
     spinstall.exe /s /v"/qn REBOOT=ReallySuppress
     ```

     ```
     REMOVE=ALL UNREGISTER_EXTENSION=1
     ```

     ```
     VCENTER_HOSTNAME=<Název hostitele nebo adresa IP nástroje vCenter>
     ```

     ```
     VCENTER_USERNAME=<jméno uživatele násroje vCenter>
     ```

     ```
     VCENTER_PASSWORD=<heslo nástroje vCenter>"
     ```

   - Odinstalujte všechny funkce pomocí instalačního programu sady:
     a. Přejděte do následujícího adresáře v instalačním programu:

     ```
     TSMVMWARE_WIN
     ```

b. Zadejte tento příkaz:

```
spinstall.exe /silent /remove
```

Poznámka: Po dokončení úplné odinstalace musíte zrušit registraci komponenty Grafické rozhraní produktu Data Protection for VMware vSphere, jak je uvedeno výše.

4. Po dokončení odinstalace restartujte systém.

Odinstalace produktu Data Protection for VMware na systému Linux

Odinstalujte produkt Data Protection for VMware a odeberte soubory a adresáře na podporovaném operačního systému Linux.

Než začnete

Chcete-li zajistit úspěšnou odinstalaci, postupujte takto:

- Odeberte uzly se serveru IBM Spectrum Protect. Musíte tak učinit před odinstalací produktu Data Protection for VMware:
  1. Spusťte příkaz dsmadmc v adresáři `/opt/tivoli/tsm/client/ba/bin/dsmadmc`.
  2. Možná budete muset použít příkaz del k odstranění souborového prostoru pro uzly: `del file` *`název_uzlu *`*
  3. Použijte příkaz q k zadání dotazu na uzly: `q filespace` *`název_uzlu *`*
  4. Použijte příkaz rem k odebrání uzlů: `rem node` *`název_uzlu`*
- Zastavte vytvořené služby dsmcad pro moduly pro přesouvání dat. Postupujte podle pokynů v technické poznámce http://www-01.ibm.com/support/docview.wss?uid=swg21358414
  1. Pomocí příkazu ps zkontrolujte, zda je spuštěna služba dsmcad: `ps -ef|grep dsmcad`
  2. Pomocí příkazu kill zastavte službu dsmcad: `kill -9` *`ID-procesu-dsmcad`*
- Musíte vyčistit soubory související s vytvořením služeb modulu pro přesouvání dat. Přejděte do instalačního adresáře a zadejte následující příkaz:

  ```
  /opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
  ```

  Stisknutím klávesy Enter vyberte název uzlu a stisknutím klávesy Enter jej odstraňte.

  Názvy uzlů naleznete v souboru `dsm.sys`
- Když odinstalujete modul IBM Spectrum Protect vSphere Client plug-in z prostředí VMware vSphere 5.5, budou odebrány pouze jeho přidružené štítky a popisky. Skutečná oprávnění zůstanou nainstalována. Tento problém je znám jako omezení VMware. Další informace viz následující článek znalostní báze VMware: http://kb.vmware.com/kb/2004601.
- Zpřístupnění souboru produktu Data Protection for VMware není po odinstalování produktu odebráno.

Informace o této úloze

Když odinstalováváte produkt Data Protection for VMware na systému Linux, je standardně typ odinstalace stejný proces jako typ původní instalace. Chcete-li použít jiný proces odinstalace, uveďte správný parametr. Pokud jste například použili proces bezobslužné instalace, můžete k odinstalování použít průvodce instalací uvedením parametru `–i swing`. Spusťte odinstalační proces jako uživatel root. Profil uživatele root musí být nalezen. Použijete-li příkaz su k přepnutí na uživatele root, použijte příkaz `su -` k nalezení profilu uživatele root.

Když začne odinstalační proces s odebíráním souborů programu, nevrátí jeho zrušení systém do čistého stavu. Tato situace může způsobit selhání pokusu o přeinstalování. V důsledku vyčistěte systém dokončením úloh, které jsou popsány v tématu “Ruční odebrání produktu Data Protection for VMware ze systému Linux” na stránce 35.

Chcete-li odinstalovat produkt Data Protection for VMware, postupujte takto:

Postup

1. Přejděte do adresáře pro odinstalační program. Výchozím umístěním odinstalačního programu je následující cesta: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. V závislosti na typu instalace, použijte jednu z následujících metod, chcete-li odinstalovat produkt Data Protection for VMware:

   Poznámka: Příkazy v této proceduře musí být zadány na jednom řádku. Tyto příklady ukazují dva řádky, aby akceptovaly formátování stránky.

   - Chcete-li použít průvodce instalací k odinstalování produktu Data Protection for VMware, zadejte tento příkaz:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
     ```

   - Chcete-li použít konzolu k odinstalování produktu Data Protection for VMware, zadejte tento příkaz:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
     ```

   - Chcete-li produkt Data Protection for VMware odinstalovat bezobslužně, zadejte tento příkaz:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
     -f uninstall.properties
     ```

     Soubor `uninstall.properties` obsahuje informace o připojení vCenter. Tyto informace jsou potřeba k odinstalaci grafického rozhraní produktu Data Protection for VMware vSphere.

Ruční odebrání produktu Data Protection for VMware ze systému Linux

Informace o této úloze

Pokud produkt Data Protection for VMware nelze odinstalovat pomocí standardní procedury odinstalace, musíte produkt Data Protection for VMware odebrat ze systému ručně, jak je popsáno v tomto postupu. Dokončete tento proces jako uživatel root.

Postup

1. Pokud jste nainstalovali komponentu Data Protection for VMware vSphere, odeberte její balík z databáze správce balíků pomocí tohoto příkazu:

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. Zadáním následujícího příkazu odeberte rozhraní API produktu IBM Spectrum Protect:

   ```
   rpm -e TIVsm-API64
   gsksslб4.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. Odeberte položky produktu z produktu Deployment Engine:

   a) Zadejte tento typ pro zobrazení seznamu všech položek:

      ```
      /usr/ibm/common/acsi/bin/de_lsrootiu.sh
      ```

   b) Chcete-li odebrat instalované jednotky položky související s produktem Data Protection for VMware, zadejte následující příkaz:

      ```
      /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <diskriminant>
      ```

      Ujistěte se, že jsou odebrány tyto položky jednotek:

      ```
      FBJRE
      TDPVMwareGUI
      ```

```
JavaHelp
TDPVMwareDM
```

Po dokončení odinstalačního programu odeberte následující adresáře, jsou-li přítomny:

- `/opt/tivoli/tsm/client`
- `/opt/tivoli/tsm/tdpvmware`

Odeberte uživatele `tdpvmware` a přidružené adresáře:

- `userdel tdpvmware`
- `/home/tdpvmware`
- `/etc/adsm`

4. Zazálohujte globální soubor registru (`/var/.com.zerog.registry.xml`).

   Po zazálohování souboru odeberte všechny značky související s produktem Data Protection for VMware.
5. Odeberte všechny soubory v instalačním adresáři (`/opt/tivoli/tsm/tdpvmware`). Odeberte také všechny zástupce umístěné na pracovní ploše.
6. Zazálohujte soubory protokolu umístěného v adresáři `/root` obsahující v názvu souboru `TDPVMware`. Například `IA-TDPVMware-00.log` nebo `IA-TDPVMware_Uninstall-00.log`.

   Po zazálohování tyto soubory protokolu odeberte. Díky jejich odebrání můžete vidět jakékoli chyby uvedené při dalším selhání instalačního procesu.
7. Nyní můžete produkt znovu nainstalovat, jak je popsáno v tématu “Instalace produktu Data Protection for VMware v systémech Linux” na stránce 22.

Úprava existující instalace produktu Data Protection for VMware

Tato sekce poskytuje pokyny pro úpravu balíků a funkcí v existující instalaci produktu Data Protection for VMware.

Pomocí instalačního programu sady můžete změnit základní balíky nainstalované na systému. Chcete-li změnit jakékoli individuální funkce balíků, můžete použít ovládací panel systému Windows **Programy a funkce**.

Úprava balíků v existující instalaci produktu Data Protection for VMware

Pomocí instalačního programu sady můžete provést změny balíků v existující instalaci produktu Data Protection for VMware.

Než začnete

Před použitím instalačního programu sady se ujistěte, že máte k dispozici zdrojové médium. Spustitelný soubor `spinstall.exe` pro instalační program sady je umístěn v kořenovém adresáři instalačního balíku.

Informace o této úloze

Pomocí instalačního programu sady můžete změnit balíky nainstalované v existující instalaci produktu Data Protection for VMware. Můžete se rozhodnout přidat nebo odebrat:

- Modul pro přesouvání dat
- Data Protection for VMware

Postupujte takto:

Postup

1. Poklepejte na soubor `spinstall.exe` a spusťte instalační balík sady.
2. Použijte zaškrtávací políčka u balíků na panelu **Vlastní nastavení** k určení balíků, které chcete nainstalovat.

3. Vyberte balíky, jejichž instalaci požadujete.

Úprava funkcí v existující instalaci produktu Data Protection for VMware

Pomocí ovládacího panelu Programy a funkce systému Windows můžete provést změny funkcí v existující instalaci produktu Data Protection for VMware.

Než začnete

Před úpravou instalačního balíku se ujistěte, že máte k dispozici zdrojové médium.

Informace o této úloze

Pomocí systém Windows upravte jednotlivé funkce balíku, které budou k dispozici v existující instalaci produktu Data Protection for VMware. Můžete se rozhodnout změnit tyto funkce:

- Modul pro přesouvání dat
- Data Protection for VMware

Postupujte takto:

Postup

1. V sekci **Programy a funkce** v **Ovládacích panelech** systému Windows klepněte pravým tlačítkem myši na volbu IBM Spectrum Protect for Virtual Environments: Aplikace Data Protection for VMware.
2. Klepněte na tlačítko **Změnit**, chcete-li aktualizovat momentálně nainstalované funkce tohoto balíku.
3. Vyberte funkce, jejichž instalaci požadujete.

Kapitola 2. Konfigurace produktu Data Protection for VMware

Tato část poskytuje pokyny pro konfiguraci produktu Data Protection for VMware a spuštění souvisejících služeb.

Tip: Po instalaci produktu Data Protection for VMware započítává IBM License Metric Tool modul pro přesouvání dat, pouze když je připojený k serveru IBM Spectrum Protect a používá se pro datové operace. Následně je modul pro přesouvání dat vždy zahrnutý do výpočtů počtů licencí. Moduly pro přesouvání dat, které nejsou připojené k serveru a nepoužívají datové operace, jsou z výpočtů počtů licencí vyloučeny.

Konfigurace nové instalace v průvodci na systému Windows

Použijte průvodce konfigurací pro počáteční konfiguraci nebo k dokončení vedlejších změn na systému Windows.

Než začnete

V případě systémů používající pouze prostředí Linux si prohlédněte téma Konfigurace nové instalace s použitím průvodce na systému Linux.

Systém, kde je nainstalován produkt Data Protection for VMware, musí mít síťovou konektivitu k následujícím serverům:

- vzdálený modul pro přesouvání dat
- server IBM Spectrum Protect
- server vCenter

Informace o této úloze

Chcete-li nakonfigurovat prostředí Data Protection for VMware, postupujte takto:

Postup

1. Otevřete webový prohlížeč a zadejte adresu webového serveru grafických rozhraní. Například:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

2. Přihlaste se pomocí jména uživatele a hesla služby vCenter.
3. V okně **Začínáme** přejděte na okno **Konfigurace** a klepněte na volbu **Spustit průvodce konfigurací**.
4. Postupujte podle instrukcí na stránkách průvodce, dokud se nezobrazí okno **Souhrn**. Přezkoumejte nastavení a klepnutím na tlačítko **Dokončit** dokončete konfiguraci a ukončete průvodce.

   Tip: Informace o každé konfigurační stránce se nachází v nápovědě online, která je nainstalována s grafickým rozhraním. Klepnutím na volbu **Další informace** v kterémkoli z oken grafického rozhraní otevřete nápovědu online pro podporu s úlohami. Viz téma *Spuštění průvodce konfigurací*.
5. Ověřte řádnou konfiguraci uzlů modulu pro přesouvání dat:
   a) Klepnutím na kartu **Konfigurace** zobrazíte stránku **Stav konfigurace**.
   b) Na stránce **Stav konfigurace** vyberte uzel modulu pro přesouvání dat a zobrazte informace o jeho stavu v podokně **Podrobnosti o stavu**.

      Když zobrazuje uzel varování nebo chybu, klepněte na něj a použijte informace v podokně **Podrobnosti o stavu** k vyřešení problému. Pak vyberte uzel a klepnutím na volbu **Ověřit vybraný uzel** ověřte, zda je problém vyřešen. Klepnutím na volbu **Obnovit** znovu otestujete všechny uzly.

Výsledky

Rychlá cesta: Po úspěšném dokončení této úlohy průvodce nejsou požadovány žádné další konfigurační úlohy pro zálohu vašich dat virtuálního počítače.

Konfigurace nové instalace pomocí průvodce na systému Linux

Použijte průvodce konfigurací pro počáteční konfiguraci nebo k dokončení vedlejších změn na systému Linux.

Než začnete

Systém, kde je nainstalován produkt Data Protection for VMware, musí mít síťovou konektivitu k následujícím serverům:

- vzdálený modul pro přesouvání dat
- server IBM Spectrum Protect
- server vCenter

Informace o této úloze

Chcete-li nakonfigurovat prostředí Data Protection for VMware na systému Linux, postupujte takto:

Postup

1. Spusťte instalační program na hostiteli Linux.
2. Vyberte volby 2 a 3 (**Modul pro přesouvání dat** a **Grafické uživatelské rozhraní**).
3. Po dokončení instalace spusťte průvodce konfigurací v tomto umístění:

   ```
   https://localhost:9081/TsmVMwareUI
   ```

   Pro snazší nastavení nadefinujte na hostiteli grafického uživatelského rozhraní pouze jeden modul pro přesouvání dat. Tento modul pro přesouvání dat musí být nakonfigurován ručně, než budete moci použít grafické uživatelské rozhraní modulu plug-in webového klienta, abyste přidali nebo nakonfigurovali další moduly pro přesouvání dat.

   Poznámka: Pokud provádíte upgrade a před upgradem jste měli fungující instanci modulu pro přesouvání dat, jednoduše restartujte služby. Nyní můžete použít modul plug-in webového klienta pro budoucí operace.
4. Během dokončování panelů v průvodci shromážděte následující informace:
   - Názvy uzlů a hesla pro registrovanou dvojici modulu pro přesouvání dat a serveru proxy pro připojení.
   - Obsah `dsm.sys` pro každý vytvořený modul pro přesouvání dat a server proxy pro připojení.
5. Po dokončení průvodce konfigurací ručně nastavte modul pro přesouvání dat, který bude spuštěn na hostiteli grafického uživatelského rozhraní.

   Přezkoumejte pro tento krok a kroky 6 a 7 informace o ručním nastavení na systému Linux v tématu Ruční nastavení uzlů modulu pro přesouvání dat v prostředí vSphere.
6. Když je spuštěná instance modulu pro přesouvání dat, ručně nastavte instanci serveru proxy pro připojení Linux, která bude spuštěna na hostiteli grafického uživatelského rozhraní.
7. Když je spuštěná instance serveru proxy pro připojení Linux, ručně nastavte instanci serveru proxy pro připojení Windows na hostiteli Windows.
8. Nyní můžete použít modul plug-in webového klienta pro budoucí operace. Starší grafické uživatelské rozhraní můžete použít, když chcete změnit nebo aktualizovat informace o výchozím serveru Spectrum Protect.

Výsledky

Rychlá cesta: Po úspěšném dokončení této úlohy průvodce nejsou požadovány žádné další konfigurační úlohy pro zálohu vašich dat virtuálního počítače.

Konfigurace prostředí s více servery

Nyní si můžete prohlédnout všechny zálohy, časové plány a operace obnovy napříč více záložními servery z jediného modulu plug-in vSphere.

Monitorujte celé prostředí ochrany dat napříč více záložními servery z jediného pohledu

Po instalaci produktu IBM Spectrum Protect můžete nakonfigurovat počáteční záložní server pomocí průvodce nastavením. Tento server je označen jako výchozí záložní server, jelikož je spuštěný jako webová aplikace na hostiteli grafického uživatelského rozhraní. Další záložní servery lze pak přidat nebo odebrat pomocí modulu plug-in. Výchozí záložní server nesmíte odebrat z modulu plug-in. Pak můžete přiřadit více záložních serverů IBM Spectrum Protect jako podporu pro datová střediska na službě vCenter. Každé datové středisko můžete přidružit k jednomu záložnímu serveru z fondu serverů Spectrum Protect. Všechny záložní servery můžete spravovat z jediného modulu vSphere nebo hostitele grafického uživatelského rozhraní produktu Data Protection for VMware.

Konfigurace výchozího záložního serveru

Po instalaci produktu IBM Spectrum Protect Data Protection for VMware můžete pomocí průvodce konfigurací nastavit počáteční výchozí záložní server.

Postup

1. Až průvodce instalací dokončí zpracování, vyberte zaškrtávací políčko **Spustit průvodce konfigurací Data Protection for VMware** a klepněte na tlačítko **Dokončit**.

   Průvodce je spuštěn ve webovém prohlížeči na následující adrese URL: `https://localhost:9081/TsmVMwareUI/`.
2. Ověřte se vůči Data Protection for VMware pomocí pověření administrátora vCenter.
3. Na kartě VMware vSphere vCenter aktualizujte podrobnosti o registraci modulu plug-in. Ujistěte sem že adresa hostitele grafického uživatelského rozhraní je platná, na kterou lze odeslat příkazy ping ze služby vCenter.
4. Na kartě **Pověření serveru** zadejte podrobnosti pro výchozí záložní server. Výchozí záložní server se použije pro webové grafické uživatelské rozhraní, kde je umístěn průvodce konfigurací (`https://localhost:9081/TsmVMwareUI/`).
5. Zvolte předponu a doménu zásad. Doporučuje se zvolit odlišnou předponu pro každý záložní server.
6. Přijměte výchozí hodnoty nebo upravte názvy na kartách **Uzel vCenter** a **Uzel VMCLI**.
7. Na stránce **Doména grafického uživatelského rozhraní** přidejte do sloupce **Spravovaná datová střediska** pouze ta datová střediska, která bude zálohovat výchozí server. Vynechte všechna datová střediska, která bude spravovat další záložní server.
8. Přijměte předvolby nebo upravte názvy na kartách **Uzly modulu pro přesouvání dat** a **Uzel serveru proxy pro připojení**. Kde je to možné si poznamenejte hesla pro uzel modulu pro přesouvání dat a uzel serveru proxy pro připojení pro jakékoli pozdější kroky ruční konfigurace.
9. V této fázi můžete volitelně nastavit obnovu souborů.
10. Přezkoumejte stránku **Souhrn** a pak dokončete proces konfigurace klepnutím na tlačítko **Dokončit**.
11. Volitelně ověřte konfiguraci přihlášením ke klientovi vSphere. Můžete přejít přímo na klienta nebo klepnout na tlačítko **Otevřít webového klienta vSphere** na obrazovce konfigurace.

Konfigurace dalších záložních serverů

Ke konfiguraci dalších záložních serverů můžete použít modul plug-in IBM Spectrum Protect vSphere.

Než začnete

Poznámka: Když konfigurujete další záložní servery pomocí modulu plug-in vSphere, musíte použít server, který podporuje protokol SSL.

Postup

1. Po dokončení počáteční konfigurace v hostiteli webového grafického uživatelského rozhraní se přihlaste k modulu plug-in a přejděte do konfigurace IBM Spectrum Protect.
2. Klepněte na volby **Konfigurovat -> Připojení** a nastavte připojení mezi modulem plug-in a hostitelem grafického uživatelského rozhraní.
3. Upravte připojení, aby ukazovalo na hostitele grafického uživatelského rozhraní.

   Po úspěšném připojení klepněte na kartu **Záložní servery**. Možná budete muset aktualizovat tabulku, abyste viděli informace o záložním serveru. Po aktualizaci se zobrazí výchozí server, který je nakonfigurovaný v hostiteli webového grafického uživatelského rozhraní.
4. Chcete-li vytvořit další záložní server, klepněte na tlačítko **+** (přidat server). Zadejte informace pro druhý server.
5. Můžete být vyzváni, abyste přijali digitální certifikáty, pokud přistupujete poprvé k rozhraní API a serveru. První certifikát ověří připojení k rozhraní REST API hostitele webového grafického rozhraní. Druhý certifikát ověří samotný nový záložní server. K tomu, abyste pokračovali, musíte přijmout oba certifikáty.
6. Vyberte doménu zásad z rozevíracího seznamu a předponu. Doporučuje se zvolit odlišnou předponu pro každý záložní server.
7. Na souhrnné obrazovce přezkoumejte své volby a přidejte záložní server klepnutím na tlačítko **Dokončit**.
8. Přidejte datové středisko klepnutím na volbu **Přidat přidružení datového střediska** v podokně **Výsledky**.
9. V sekci **Správa datového střediska** přezkoumejte seznam všech datových středisek v konkrétní službě vCenter. Vyberte datové středisko, které má být přidruženo k záložnímu serveru. Přidružte záložní server k datovému středisku klepnutím na volbu **Vytvořit přidružení**.
10. Klepněte na volbu **Vytvořit přidružení** a zadejte podrobnosti serveru, který musí být přidružen k datovému středisku.
11. Přidejte modul pro přesouvání dat pro datové středisko. Každé datové středisko vyžaduje svůj vlastní modul pro přesouvání dat. Avšak stejnou instalaci modulu pro přesouvání dat lze použít pro více datových středisek. Přejděte přímo do podokna modulu pro přesouvání dat výběrem volby **Přidat modul pro přesouvání dat**.
12. Klepněte na volbu **Přidat modul pro přesouvání dat** na kartě **Moduly pro přesouvání dat**. Hostitel modulu pro přesouvání dat může být na hostitelském počítači grafického uživatelského rozhraní. Další volbou je instalovat modul pro přesouvání dat odděleně.
13. Po přidání prvního modulu pro přesouvání dat do datového střediska se automaticky vytvoří časový plán.
14. Klepněte na volby **Konfigurovat -> Časové plány**. Aktualizujte tabulku časových plánů, abyste viděli nový časový plán.

    Další záložní server je nyní nakonfigurován pro použití produktem Data Protection for VMware.

Vytvoření časových plánů s dalšími záložními servery

Po nastavení výchozího záložního serveru použijte modul plug-in IBM Spectrum Protect vSphere ke konfiguraci dalších záložních serverů.

Než začnete

Počáteční výchozí časový plán nemá žádný objekt. Časový plán musí mít označený objekt ke spuštění záloh.

Informace o této úloze

Poté, co nakonfigurujete jeden nebo více záložních serverů, můžete vytvořit výchozí časový plán. Tento časový plán můžete použít k nadefinování dalších záložních serverů. Pokud jsou vyžadovány další časové plány, postupujte podle pokynů v tématu Vytvoření časového plánu, který je kompatibilní se značením.

Každý časový plán je přidružen ke konkrétnímu datovému středisku. Každý časový plán může mít jeden nebo více modulů pro přesouvání dat.

Postup

1. Chcete-li přidat objekt pro časový plán pro zálohování, přejděte na datové středisko, které je přidružené k tomuto časovému plánu. Vyberte objekt na úrovni datového střediska nebo na nižší úrovni, klepněte pravým tlačítkem myši na objekt a klepněte na volbu **IBM Spectrum Protect -> Konfigurovat ochranu dat**.
2. V podokně **Konfigurovat zásady zálohování** vyberte nový časový plán, aby se spustila záloha daného objektu.
3. Po přidružení objektu ověřte následující položky:
   - Ověřte, že objekt zobrazuje správné informace, když klepnete na obrzovku **Konfigurovat -> IBM Spectrum Protect**.
   - Ověřte, že je v časovém plánu nyní uveden vybraný objekt, když klepnete na volby **Nabídka -> IBM Spectrum Protect -> Konfigurovat -> Časové plány**.
   - Po spuštění časového plánu přejděte na objekt a klepněte na volby **Monitorovat -> IBM Spectrum Protect**.

   Rada: Volitelně, chcete-li aktualizovat čas zahájení časového plánu z příkazového řádku, proveďte následující akce:

   a. Přejděte do umístění dsmadmc: `C:/Program Files/Tivoli/TSM/baclient`
   b. V příkazovém řádku vyhledejte soubor `dsm*opt` modulu pro přesouvání dat, který je přidružený k danému serveru. (`dir * opt`)
   c. Zadejte příkaz `dsmadmc - optfile=dsm.datamovername.opt`.
   d. Chcete-li spustit časový plán za 10 minut, zadejte tento příkaz:

      ```
      update schedule policyDomain scheduleName StartTIME=NOW+00:10
      ```

Spuštění jednorázových záloh

Když je dokončena konfigurace pro více záložních serverů IBM Spectrum Protect, můžete spustit jednorázové zálohy.

Postup

1. Vyberte datové středisko, které je přidruženo ke konkrétnímu serveru, na kterém chcete testovat zálohy. Přejděte na objektu uvnitř daného datového střediska, klepněte na něj pravým tlačítkem a klepněte na volbu **Zálohovat**.
2. Vyberte požadované volby a zahajte zálohování klepnutím na tlačítko **Spustit**.
3. Volitelně můžete monitorovat průběh v tabulce **Nejnovější úlohy** vSphere.
4. Po dokončení zálohy můžete volitelně zkontrolovat stav tak, že vyberete zálohu objektu a pak klepnete na volby **Monitorovat -> IBM Spectrum Protect**.

Spuštění jednorázových operací obnovy

Poté, co byl virtuální počítač zálohován na server IBM Spectrum Protect, můžete spustit jednorázové operace obnovy.

Postup

1. Určete, které virtuální počítače mají zálohy, výběrem datového střediska a zvolením volby **Monitorovat -> IBM Spectrum Protect**.

   Zobrazí se tabulka se seznamem všech virtuálních počítačů a jejich stavem zálohy.
2. Vyberte virtuální počítač se zálohou v inventáři a klepněte pravým tlačítkem myši na **IBM Spectrum Protect -> Obnovit**.

3. Vyberte bod obnovení a uveďte jakékoli další volby.
4. Po dokončení průvodce obnovením klepněte na tlačítko **Dokončit**.
5. Volitelně monitorujte průběh obnovení pomocí pohledu **Nedávné úlohy** ve vSphere.
6. Volitelně ověřte stav operace obnovení v inventáři.

Použití zápisníku pro úpravu existující instalace

Pomocí zápisníku Upravit konfiguraci upravíte existující nastavení konfigurace.

Než začnete

Zápisník Upravit konfiguraci poskytuje pro existující konfiguraci následující úlohy:

- Nastavte nebo změňte ID administrátora produktu IBM Spectrum Protect.
- Resetujte heslo a odemkněte uzel VMCLI.
- (prostředí vSphere) Přidání nebo odebrání datových středisek VMware do domény grafického rozhraní produktu Data Protection for VMware vSphere.
- Přidejte nebo odeberte uzly serveru proxy připojení. Upravte heslo pro existující uzel serveru proxy připojení.
- Přidání nebo odebrání uzlu modulu pro přesouvání dat. Upravte heslo pro existující uzel modulu pro přesouvání dat.
- Povolte obnovu souborů.
- Povolte podporu značení pro uzel modulu pro přesouvání dat.

Informace o této úloze

Chcete-li upravit existující konfiguraci, postupujte takto:

Postup

1. Otevřete webový prohlížeč a zadejte adresu webového serveru grafických rozhraní.
   Například:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   Přihlaste se pomocí jména uživatele a hesla služby vCenter.
2. V okně **Začínáme** přejděte na okno **Konfigurace** a klepněte na volbu **Upravit konfiguraci**.
3. Přejděte na stránku příslušnou vaší úloze úpravy a postupujte podle instrukcí. Musíte klepnout na tlačítko **OK** pro uložení změn, než přejdete na jinou stránku **Nastavení konfigurace**. Jinak se změny neprojeví.

   Důležité: Informace o každé konfigurační stránce se nachází v nápovědě online, která je nainstalována s grafickým rozhraním. Klepnutím na volbu **Další informace** v kterémkoli z oken grafického rozhraní otevřete nápovědu online pro podporu s úlohami. Prohlédněte si téma *Úprava existující konfigurace*.

Výsledky

Aktualizovaná nastavení se zobrazí v okně **Konfigurace**.

Windows Povolení prostředí pro operace obnovy souborů

Když administrátor povolí funkci obnovy souborů, mohou vlastníci souborů obnovovat soubory bez asistence.

Než začnete

Pokud jste neověřili, zda jsou splněny všechny předpoklady, přezkoumejte téma o předpokladech pro obnovení souborů v uživatelské příručce *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide*.

Informace o této úloze
V systému, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere, postupujte takto.

Postup

1. Spusťte grafické rozhraní produktu Data Protection for VMware vSphere otevřením webového prohlížeče a zadáním adresy webového serveru grafických rozhraní.
   Například:

   ```
   https://<adresa webového serveru grafických rozhraní>:9081/TsmVMwareUI/
   ```

   Přihlaste se pomocí ID uživatele a hesla vCenter.
2. V okně **Začínáme** klepněte na volbu **Konfigurace** a vyberte jednu z následujících úloh ze seznamu **Úlohy**:
   - Pokud konfigurujete nové prostředí, postupujte takto:
     a. Vyberte volbu **Spustit průvodce konfigurací klienta**.
     b. Postupujte podle pokynů na každé stránce průvodce. Pomocí následujícího návodu dokončíte stránku **Obnova souboru**:
        1) Vyberte volbu **Povolit obnovu souborů**.
        2) Zadejte kontaktní informace administrátora, které se zobrazí v rozhraní obnovy souborů. Pokud nechcete kontaktní informace poskytnout, vymažte zaškrtávací políčko.
        3) Pokud prostředí obsahuje zálohy virtuálních počítačů Windows, zadejte pověření uživatele domény Windows. Jinak zaškrtávací políčko vymažte a nezadávejte žádná pověření.

           Tip: Operace obnovy souboru používá pověření uživatele domény Windows pro přístup k síťovým sdíleným složkám na vzdáleném virtuálním počítači. Pokud prostředí obsahuje zálohy virtuálních počítačů Windows a nejsou zadána žádná pověření nebo nesprávná pověření, operace selže. Proto vymažte toto zaškrtávací políčko, pouze pokud nemáte žádné zálohy virtuálních počítačů Windows.
        4) Klepnutím na adresu URL rozhraní pro obnovení souboru ověřte dostupnost rozhraní.

           Zapamatujte si: Uložte si adresu URL rozhraní pro obnovení souborů. Vlastník virtuálního počítače hosta bude k rozhraní pro obnovení souborů přistupovat přes tuto adresu URL.
        5) Klepnutím na tlačítko **OK** uložte změny.
   - Pokud aktualizujete existující prostředí, postupujte takto:
     a. Vyberte volbu **Upravit konfiguraci TSM**.
     b. Na stránce **Obnova systému** postupujte takto:
        1) Vyberte volbu **Povolit obnovu souborů**.
        2) Zadejte kontaktní informace administrátora, které se zobrazí v rozhraní obnovy souborů. Pokud nechcete kontaktní informace poskytnout, vymažte zaškrtávací políčko.
        3) Pokud prostředí obsahuje zálohy virtuálních počítačů Windows, zadejte pověření uživatele domény Windows. Jinak zaškrtávací políčko vymažte a nezadávejte žádná pověření.

           Tip: Operace obnovy souboru používá pověření uživatele domény Windows pro přístup k síťovým sdíleným složkám na vzdáleném virtuálním počítači. Pokud prostředí obsahuje zálohy virtuálních počítačů Windows a nejsou zadána žádná pověření nebo nesprávná pověření, operace selže. Proto vymažte toto zaškrtávací políčko, pouze pokud nemáte žádné zálohy virtuálních počítačů Windows.
        4) Klepnutím na adresu URL rozhraní pro obnovení souboru ověřte dostupnost rozhraní.

           Zapamatujte si: Uložte si adresu URL rozhraní pro obnovení souborů. Vlastník virtuálního počítače hosta bude k rozhraní pro obnovení souborů přistupovat přes tuto adresu URL.
        5) Klepnutím na tlačítko **OK** uložte změny.

Výsledky

V prostředí je nyní povoleno provádět operace obnovení souborů. Vlastníci souborů mohou obnovit své soubory, když přistoupí na adresu URL rozhraní obnovy souborů produktu IBM Spectrum Protect.

Linux Nastavení operací obnovy souboru na systému Linux

Chcete-li povolit funkci obnovy souboru, pokud je produkt Data Protection for VMware nainstalován na systému Linux, musí být nastaveno další prostředí Data Protection for VMware v systému Windows.

Informace o této úloze

Když spustíte produkt Data Protection for VMware v prostředí systému Linux, funkce obnovy souboru musí být nainstalována na systému Windows, aby byla povolena.

Postup

1. Nastavte oddělený server Windows, který se použije pro funkci obnovy souborů.
2. Nainstalujte produkt Data Protection for VMware na systém Windows. Přijměte výchozí hodnoty během instalace.
3. Když nakonfigurujete produkt Data Protection for VMware v systému Windows, použijte následující názvy uzlů:
   a) Vytvořte uzel vCenter nazvaný `VCENTER_FR`.
   b) Vytvořte uzel VMCLI nazvaný `VMCLI_FR`.
   c) Opětovně použijte název uzlu datového střediska z prostředí systému Linux.
   Například: `DATACENTER`.
   d) Nevytvářejte uzel modulu pro přesouvání dat. Uzel modulu pro přesouvání dat není vyžadován pro funkci obnovy souborů v tomto scénáři.
   e) Vytvořte následující novou dvojici uzlů serverů proxy připojení nazvanou `REMOTE_FR_MP_WIN` a `REMOTE_FR_MP_LNX`.
4. Na stránce **Obnova souborů** v průvodci konfigurací vyberte volbu `Povolit obnovu souborů`.
5. Chcete-li získat přístup k rozhraní pro obnovu souborů, otevřete webový prohlížeč a zadejte adresu URL, kterou vám poskytl administrátor.
   Například:

   ```
   https:\\hostname:9081\FileRestoreUI
   ```

   kde `hostname` je název hostitele systému Windows, kde je nainstalován produkt Data Protection for VMware.

Výsledky

Následující příklad ukazuje relace uzlu serveru proxy na serveru IBM Spectrum Protect:

```
tsm: SERVER>q proxy

Cílový uzel       Uzel agenta
---------------     ---------------------------------------------
VCENTER             VMCLI DATACENTER
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

Další uzly, které jsou vytvořeny pro povolení funkce obnovy souborů, mají příponu _FR.

Windows Úprava voleb pro operace obnovy souboru

Chcete-li administrátorům umožnit konfigurovat a řídit zpracování obnovy pro operace obnovení souboru, upravte volby v souboru `frConfig.props`.

Informace o této úloze
V systému, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere, postupujte takto.

Postup

1. Přejděte do adresáře, kde je umístěn soubor `frConfig.props`.
   Otevřete například příkazový řádek a zadejte tento příkaz:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. Otevřete soubor `frConfig.props` pomocí textového editoru v režimu administrátora a upravte volby dle potřeby.

   Pomocí informací v produktu "Volby obnovy souboru" na stránce 47 určíte, které volby upravit.
3. Uložte změny a zavřete soubor `frConfig.props`.

Výsledky
Upravené volby se použijí pro rozhraní pro obnovu souborů IBM Spectrum Protect.

Volby obnovy souboru

Konfigurace řízení voleb `frConfig.props`, podpora a zpracování obnovení pro operace obnovení souboru.

enable_contact_info=false | true
Uveďte, zda chcete poskytnout kontaktní informace na administrátora, které vlastníci souborů mohou použít, aby získali podporu.

false
Vlastníci souborů neobdrží kontaktní informace na administrátora. Tato hodnota je předvolba.

true
Vlastníci souborů obdrží kontaktní informace na administrátora.

Pokud uvedete parametr **enable_contact_info=true**, musíte poskytnout informace ve volbě **contact_info**.

enable_filerestore=false | true
Uveďte, zda mohou vlastníci souboru obnovit své soubory z virtuálního počítače pomocí rozhraní pro obnovu souborů IBM Spectrum Protect.

false
Vlastníci souborů nemohou obnovit své soubory pomocí rozhraní pro obnovu souborů IBM Spectrum Protect. Tato hodnota je předvolba.

true
Vlastníci souborů mohou obnovit své soubory pomocí rozhraní pro obnovu souborů IBM Spectrum Protect.

maximum_mount_points=*num_mount_points*
Uveďte maximální počet souběžných bodů obnovy, které jsou k dispozici uživatelskému účtu. Minimální hodnota je 1 bod obnovy. Maximální hodnota je 256 bodů připojení. Výchozí hodnota je 2 body připojení.

Tip: Chcete-li zabránit virtuálnímu počítači, aby byl připojován několikrát pro simultánní operace obnovy, nastavte tuto volbu na nízkou hodnotu.

mount_session_timeout_minutes=*num_mins*
Uveďte dobu, v minutách, jak dlouho mohou být obnova a připojený bod obnovy nečinné, než bude relace zrušena. Zrušení odpojí bod obnovy. Maximální hodnota je 8 hodin (480 minut). Výchozí hodnota je 30 minut.

Tip: Chcete-li zabránit neočekávanému zrušení relace, zvyšte počet minut.

restore_info_duration_hours=*num_hrs*
Uveďte dobu, v hodinách, jak dlouho jsou zachovány informace o nedávné aktivitě obnovy v rozhraní pro obnovu souborů IBM Spectrum Protect. Okno obnovení aktivity použijte k zobrazení informací o chybě a nedávno dokončených úlohách. Tyto informace poskytují způsob, jak vyhledat nedávno obnovené soubory. Maximální hodnota je 14 dnů (336 hodin). Výchozí hodnota je jeden týden (168 hodin).

contact_info=*administrator information*
Zadejte kontaktní informace na administrátora, které mohou použít vlastníci souborů pro získání podpory. Kontaktní informace se zobrazí v rozhraní pro obnovu souborů produktu IBM Spectrum Protect v následujících umístěních:

- přihlašovací okno
- podokno **O produktu** v nabídce nápovědy
- odkaz na informace o podpoře ve zprávách o rozhraní

Následující volby můžete přepsat pomocí průvodce konfigurací grafického rozhraní produktu Data Protection for VMware vSphere nebo pomocí zápisníku:

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

Konfigurace aktivity protokolování pro operace obnovy souborů

Chcete-li administrátorům umožnit konfigurovat a řídit, jak je formátován obsah zaprotokolován pro operace obnovy souborů, upravte volby v souboru FRLog.config.

Než začnete

Soubor FRLog.config se vygeneruje poprvé, kdy je přistoupeno k rozhraní pro obnovu souborů IBM Spectrum Protect.

Informace o této úloze

V systému, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere, postupujte takto.

Postup

1. Přejděte do adresáře, kde je umístěn soubor FRLog.config.
   Otevřete příkazový řádek a zadejte následující příkaz:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```

2. Otevřete soubor FRLog.config pomocí textového editoru v režimu administrátora a upravte volby dle potřeby.

   Pomocí informací v produktu “Volby aktivit protokolu obnovy souboru” na stránce 49 určíte, které volby upravit.
3. Uložte změny a zavřete soubor FRLog.config.
4. Restartujte webový server grafického rozhraní:
   a) Klepněte na nabídku **Start** > **Ovládací panel** > **Administrativní nástroje** > **Služby**.
   b) Klepněte pravým tlačítkem myši na nabídku **Data Protection for VMware Web Server Service** a klepněte na volbu **Restart**.

Výsledky

Nastavení se použijí na obsah a formát zaprotokolovaných informací pro operace obnovení souboru.

Volby aktivit protokolu obnovy souboru

Volby FRLog.config řídí obsah a formát zaprotokolovaných informací pro operace obnovení souboru.

Následující volby zaznamenávají informace pro úlohy obnovy souboru v souboru fr_gui.log:

MAX_LOG_FILES=*počet*
Uveďte maximální počet souborů fr_gui.log, které budou zachovány. Výchozí hodnota je 8.

MAX_LOG_FILE_SIZE=*číslo*
Zadejte maximální velikost souboru fr_gui.log v KB. Výchozí hodnota je 8192 KB.

Následující volby zaznamenávají informace pro služby obnovy souborů v souboru fr_api.log. Tyto služby jsou interní služby rozhraní API, které souvisí s aktivitou obnovy souborů:

API_MAX_LOG_FILES=*počet*
Uveďte maximální počet souborů fr_api.log, které budou zachovány. Výchozí hodnota je 8.

API_MAX_LOG_FILE_SIZE=*číslo*
Zadejte maximální velikost souboru fr_api.log v KB. Výchozí hodnota je 8192 KB.

API_LOG_FILE_NAME=*název_souboru_protokolu_API*
Uveďte název souboru protokolu rozhraní API. Výchozí hodnota je fr_api.log.

API_LOG_FILE_LOCATION=*název_souboru_protokolu_API*
Uveďte umístění souboru protokolu rozhraní API. Umístění musí být uvedeno pomocí dopředného lomítka (/). Výchozí umístění je C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs.

FR.API.LOG=ON | OFF
Uveďte, zda povolit protokolování pro služby obnovy souborů.

- Chcete-li povolit služby obnovy souborů, zadejte hodnotu ON. Výchozí hodnota je ON.
- Chcete-li zakázat protokolování služeb obnovy souborů, zadejte OFF.

Chcete-li odstranit problémy, s nimiž se můžete setkat při operacích obnovy souborů, prohlédněte si téma Volby trasování pro obnovu souborů. Volby trasování jsou také uvedeny v souboru FRLog.config.

Konfigurace podpory značení na uzlu modulu pro přesouvání dat

Když je na uzlu modulu pro přesouvání dat povolena podpora značení, mohou administrátoři používat značky ochrany dat pro objekty stavu zásob v datovém středisku VMware vCenter.

Než začnete

Ověřte, že jsou splněny následující požadavky:

- Server VMware vCenter musí být ve verzi 6.0, aktualizace 1 nebo pozdější.
- Aby grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere správně fungovalo s podporou značení, ujistěte se, že jsou během instalace grafického uživatelského rozhraní splněny následující požadavky:
  - Alespoň jeden modul pro přesouvání dat a grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere musí být nainstalováno na stejném serveru. Tento uzel modulu pro přesouvání dat musí být nakonfigurován, aby se uložila pověření serveru vCenter. Pověření můžete uložit spuštěním průvodce konfigurací, který uloží heslo uzlu modulu pro přesouvání dat, nebo použitím příkazu **dsmc set password** v příkazovém řádku modulu pro přesouvání dat.

    Pokud používáte jiné moduly pro přesouvání dat, spuštěné na virtuálních počítačích nebo fyzických počítačích jako dodatečné moduly pro přesouvání dat, můžete je nainstalovat na jiných serverech. Kvůli podpoře značení musí mít všechny tyto moduly pro přesouvání dat také nakonfigurovanou volbu VMTAGDATAMOVER YES. Tyto dodatečné moduly pro přesouvání dat nevyžadují instalaci grafického rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere na stejném serveru, aby správně fungovaly jako moduly pro přesouvání dat založené na značkách.
  - Linux

V případě modulů pro přesouvání dat Linux se ujistěte, že uvedete instalační adresář modulu pro přesouvání dat a sdílenou knihovnu JavaTM `libjvm.so` v proměnné prostředí `LD_LIBRARY_PATH`. Cesta k souboru `libjvm.so` se používá pro podporu značení, když povolíte volbu `vmtagdatamover` v modulu pro přesouvání dat. Počínaje verzí 8.1.8 byl přidán nový skript (`spve.sh`) do `/etc/profile.d`. Tím se správně nastaví cesta `LD_LIBRARY` pro následující aplikace: `dsmc`, `dsmcad` a `dsmj`. Toto by mělo také zahrnout `libjvm.so`. Pokud uvidíte chyby s proměnnou `LD_LIBRARY_PATH`, postupujte podle ručních pokynů:

1. IBM Java:

   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
   ```

   Oracle Java:

   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
   ```

2. Chcete-li nakonfigurovat služby Client Acceptor Service a Data Mover Scheduler Service, aby sloužily jako záložní server vStorage, nastavte v souboru `/etc/init.d/dsmcad` následující proměnnou prostředí:

   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   ```

Poznámka: V operačních systémech Linux musí být instalováno grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere pomocí výchozího jména uživatele (`tdpvmware`).

– Na klientech UNIX a Linux jsou existující hesla v souborech `TSM.PWD` migrována do nového úložiště hesel ve stejném umístění. Výchozí umístění úložiště hesel pro uživatele root je `/etc/adsm`. Umístění úložiště hesel jiných uživatelů než root je uvedeno ve volbě `passworddir`.

  Soubor `TSM.PWD` je po migraci odstraněn.

Poznámka: Další informace k používání oprávnění požadovaných pro práci se značením naleznete v části Instalace komponent Data Protection for VMware

Informace o této úloze

Značky ochrany dat můžete použít ke konfiguraci zásad zálohování virtuálních počítačů do objektů zásob VMware. Tyto značky ochrany dat se ukazují jako nastavení, která lze změnit v modulu IBM Spectrum Protect vSphere Client plug-in.

Procedura

- Použijte jednu z těchto metod:

Volba	Popis
Konfigurace uzlu modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere	1. V modulu vSphere vyberte IBM Spectrum Protect . 2. Na kartě **Konfigurovat** vyberte volbu **Moduly pro přesouvání dat**. 3. Na panelu **Přidat modul pro přesouvání dat** vyberte datové středisko v rozevírací nabídce. 4. Přijměte předvolby, nebo upravte nastavení polí **Název modulu pro přesouvání dat**, **Název hostitele modulu pro přesouvání dat**, **Uživatele služby vCenter** a **Heslo služby vCenter**. 5. Po dokončení nastavení klepněte na tlačítko **Přidat**. Další podrobnosti naleznete v tématu "Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere" v instalační příručce produktu Grafické rozhraní produktu Data Protection for VMware vSphere.

Volba	Popis
Chcete-li konfigurovat podporu značení na *novém* modulu pro přesouvání dat na systému Windows nebo Linux pomocí grafického rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere	1. Na systému, kde je nainstalováno grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere, spusťte grafické rozhraní otevřením webového prohlížeče a zadáním adresy webového serveru grafického rozhraní. Například: `https://<adresa webového serveru grafických rozhraní>:9081/TsmVMwareUI/` 2. Přihlaste se pomocí ID uživatele a hesla vCenter. 3. Přejděte na kartu **Konfigurace** a vyberte akci **Upravit IBM Spectrum Protect konfiguraci**. 4. Přejít na stránku **Uzly modulu pro přesouvání dat** zápisníku konfigurace. 5. Přidejte uzel modulu pro přesouvání dat pomocí následujícího postupu: a. Pro uzel modulu pro přesouvání dat, pro který chcete nastavit podporu značení, vyberte volbu **Vytvořit služby**. Standardně je vybrána volba **Uzel založený na značce**, která umožní podporu značení na uzlu modulu pro přesouvání dat. b. Chcete-li označit uzel založený na značce jako výchozí uzel modulu pro přesouvání dat, vyberte volbu **Výchozí modul pro přesouvání dat**. Výchozí uzel modulu pro přesouvání dat zálohuje všechny nové virtuální počítače přidané do libovolného kontejneru v datovém středisku, pokud je kontejner již součástí ochranné sady. Výchozí modul pro přesouvání dat také zálohuje všechny virtuální počítače v ochranné sadě, které nemají přiřazenou značku `Modul pro přesouvání dat`. **Tip:** Pokud na systémech Linux zvolíte nový uzel modulu pro přesouvání dat jako výchozí uzel značení, odeberte řádek `vmtagdefaultdatamover` ze všech ostatních souborů voleb modulu pro přesouvání dat, které jsou přidruženy k tomuto datovému středisku. c. Klepnutím na tlačítko **OK** uložte změny. Volby `vmtagdatamover` a `vmtagdefaultdatamover` (jsou-li nastaveny) se přidají do souboru voleb modulu pro přesouvání dat (`dsm.opt`).
Chcete-li konfigurovat podporu značení pro *existující* uzel modulu pro přesouvání dat systému Windows, pokud se uzel nachází na stejném serveru jako grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere	1. Proveďte kroky 1-3 z předchozího postupu a nakonfigurujte podporu značení na novém uzlu modulu pro přesouvání dat. 2. Na stránce **Uzly modulu pro přesouvání dat** vyberte volbu **Uzel založený na značce** pro uzel, pro který chcete povolit podporu značení. 3. **Volitelné:** Chcete-li označit uzel založený na značce jako výchozí uzel modulu pro přesouvání dat, vyberte volbu **Výchozí modul pro přesouvání dat**.
Chcete-li konfigurovat podporu značení na *existujícím* uzlu modulu pro přesouvání dat	1. Přidejte volbu `vmtagdatamover yes` do souboru voleb modulu pro přesouvání dat (`dsm.sys` pro systém Linux a `dsm.opt` pro systém Windows).

Volba	Popis
systému Linux nebo na existujícím uzlu modulu pro přesouvání dat systému Windows, který se nachází na jiném serveru než grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere	2. **Volitelné:** Chcete-li označit uzel založený na značce jako výchozí uzel modulu pro přesouvání dat, přidejte volbu `vmtagdefaultdatamover yes` nebo `vmtagdefaultdatamover` *dm_name* do souboru voleb modulu pro přesouvání dat. **Tip:** Pokud na systémech Linux zvolíte nový uzel modulu pro přesouvání dat jako výchozí uzel značení, odeberte řádek `vmtagdefaultdatamover` ze všech ostatních souborů voleb modulu pro přesouvání dat, které jsou přidruženy k tomuto datovému středisku.

Výsledky

Až bude uzlu modulu pro přesouvání dat povolena podpora značení, bude se modul pro přesouvání dat dotazovat inventáře VMware na informace o značení, když spustí zálohu. Modul pro přesouvání dat poté zazálohuje virtuální počítače na základě značek ochrany dat, které byly nastaveny. Pokud není na uzlu modulu pro přesouvání dat nakonfigurována podpora značení, značky ochrany dat se budou během operace zálohování ignorovat.

Související informace

`Vmtagdatamover`
`Vmtagdefaultdatamover`
Konfigurace zásad zálohování

Konfigurace prostředí pro operace úplné okamžité obnovy virtuálního počítače

Nastavte vyhrazenou síť iSCSI pro úplnou okamžitou obnovu virtuálního počítače a operace okamžitého přístupu.

Než začnete

Použijte příslušnou dokumentaci VMware (ESXi nebo vSphere), chcete-li určit konkrétní kroky, které je třeba provést pro konfiguraci virtuálního přepínače iSCSI a sítě virtuálních počítačů. Ačkoliv jsou poskytnuty obecné pokyny, specifická dokumentace a vysvětlení toho, jak přidat virtuální sítě a virtuální přepínače, jsou mimo rozsah dokumentace k produktu. V době publikace příručky je k dispozici dokumentace k produktu verze VMware vSphere ESXi a vCenter 5.5 v sekci Dokumentace k produktu VMware ESXi a vCenter Server 5. Témata “Provoz sítě” obsahují informace pro přidání a konfiguraci virtuálních přepínačů a virtuálních sítí.

Důležité: Tato nastavení konfigurace jsou poskytnuta jako pomoc s nastavením prostředí VMware pro efektivní úplnou okamžitou obnovu virtuálního počítače a operace okamžitého přístupu. Nicméně vzhledem k tomu, že se tato nastavení použijí na konfigurační úlohy VMware a uživatelská rozhraní VMware, musíte se obrátit na příslušnou dokumentaci VMware, kde najdete podrobné pokyny, krok za krokem.

Informace o této úloze

Tato procedura vyžaduje adaptér iSCSI na každém hostiteli ESXi, který se používá pro operace okamžité obnovy. K nastavení adaptéru použijte odpovídající dokumentaci VMware. V době publikace jsou k dispozici následující postupy k tomuto prostředku VMware vSphere.

- Chcete-li nastavit softwarový adaptér iSCSI, postupujte podle pokynů v proceduře VMware “Konfigurovat softwarové adaptéry iSCSI”.
- Chcete-li nastavit adaptér iSCSI, postupujte podle pokynů v proceduře VMware “Nastavení nezávislých hardwarových adaptérů iSCSI”.

1. Konfigurace softwaru iSCSI na hostiteli ESXi

Postup

Tato úloha nastaví software iSCSI pro základní konfiguraci.

1. Přihlaste se k hostiteli ESXi, který se použije pro operace okamžité obnovy.
2. Postupujte podle pokynů v tomto článku znalostní báze VMware, dokud nebude povolen adaptér iSCSI:

   http://kb.vmware.com/kb/1008083
   Produkt IBM Spectrum Protect automaticky zjistí cílový server iSCSI.
3. Ověřte, že adresa IP adaptéru iSCSI (na hostiteli ESXi) je stejná adresa podsítě, která je použitá pro modul pro přesouvání dat.
4. Ověřte, že licence Storage vMotion je na hostiteli ESXi povolena.

Jak pokračovat dále
Po nastavení softwaru iSCSI na hostiteli ESXi, nainstalujte a nakonfigurujte aplikace na systému modulu pro přesouvání dat.

2. Instalace a konfigurace aplikací v modulu pro přesouvání dat

Než začnete
Je-li na systému modulu pro přesouvání dat již nainstalován a nakonfigurován agent zotavení a modul pro přesouvání dat IBM Spectrum Protect, začněte krokem 3.

Postup

Tato úloha nastaví systém modulu pro přesouvání dat s aplikacemi a nastaveními pro operace okamžité obnovy.

1. Nainstalujte agenta zotavení a modul pro přesouvání dat IBM Spectrum Protect na systému modulu pro přesouvání dat.

   V kroku 4 procedury Instalace produktu Data Protection for VMware vyberte typ instalace **Instalovat úplný modul pro přesouvání dat pro ochranu hostovaných aplikací**.
2. Nakonfigurujte modul pro přesouvání dat.

   Postupujte podle pokynů v tématu "Konfigurace modulu pro přesouvání dat" v dokumentaci klienta.
3. Nastavte adresu IP serveru iSCSI:
   a) Přejděte do souboru `C:\Program Files\Tivoli\TSM\baclient\dsm.opt` a uveďte následující parametr:

   ```
   VMISCSIServeraddress=<adresa IP síťové karty v systému modulu
   pro přesouvání dat,
   který vystaví cíle iSCSI.>
   ```

   Pokud má váš systém modulu pro přesouvání dat více než jednu síťovou kartu, ujistěte se, že pro síť iSCSI uvedete správnou síťovou kartu.

Jak pokračovat dále
Po nastavení systému modulu pro přesouvání dat zaveďte připojení mezi rozhraním příkazového řádku agenta zotavení a grafickým rozhraním agenta zotavení.

3. Nastavení připojení agenta zotavení

Než začnete
Rozhraní příkazového řádku agenta zotavení (CLI) V7.1.x lze zobrazit jako rozhraní API příkazového řádku do grafického rozhraní agenta zotavení. Rozhraní příkazového řádku agenta zotavení můžete použít ke komunikaci s grafickým rozhraním agenta zotavení.

Postup

Tato úloha zavede připojení mezi rozhraním příkazového řádku agenta zotavení a grafickým rozhraním agenta zotavení.

1. Spusťte rozhraní příkazového řádku agenta zotavení na systému modulu pro přesouvání dat.

   V nabídce **Start systému Windows** klepněte na volby **Programy** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**.
2. V okně příkazového řádku zadejte tento příkaz:

   ```
   RecoveryAgentShell.exe -c set_connection mount_computer <Adresa IP
   síťové karty v systému modulu pro přesouvání dat, který vystavuje cíle iSCSI.>
   ```

   Tento příkaz zavede připojení mezi rozhraním příkazového řádku agenta zotavení a grafickým rozhraním agenta zotavení.

Jak pokračovat dále
Po zavedení připojení nakonfigurujte vyhrazenou síť iSCSI.

4. Konfigurace vyhrazené sítě iSCSI pro hostitele ESXi a modul pro přesouvání dat

Než začnete
Přezkoumejte tyto pokyny, než budete pokračovat s touto úlohou:

- Použijte vyhrazenou síť iSCSI pro operace okamžité obnovy.
- Každý hostitel ESXi, který se používá pro operace okamžité obnovy, musí mít k dispozici druhou fyzickou síťovou kartu. Tato druhá síťová karta je vázána na softwarový adaptér iSCSI odpovídajícího hostitele ESXi.
- Systém modulu pro přesouvání dat, který je spuštěn na virtuálním počítači, musí mít k dispozici druhou síťovou kartu. Tato druhá síťová karta je vázána na softwarový adaptér iSCSI hostitele ESXi.
- Každý hostitel ESXi, který se používá pro operace okamžité obnovy, musí mít k dispozici sekundární datové úložiště VMware. Toto dočasné datové úložiště obsahuje informace o konfiguraci a data virtuálního počítače vytvořená během operace.

Postup

Tato úloha nastaví vyhrazenou síť iSCSI pro hostitele ESXi a pro modul pro přesouvání dat, který je spuštěn na virtuálním počítači.

1. Přihlaste se k hostiteli ESXi, který se použije pro operace okamžité obnovy.
2. Nastavte virtuální přepínač pro síť iSCSI.

   Tyto kroky jako virtuální přepínač používají *vSwitch1*.
   a) Vyberte volbu **Síťový adaptér VMkernel** pro **Typ připojení**.

      Síť iSCSI vyžaduje tento typ připojení.
   b) Vyberte volbu **Vytvořit standardní přepínač vSphere** pro **Síťový přístup VMkernel**.
   c) Vyberte volbu **Popisek sítě** pro **Nastavení připojení VMkernel**.

      Zadejte štítek, který označuje, že přepínač *vSwitch1* a tato síť jsou pro váš přenos iSCSI.

      Například: *VMkernel iSCSI*.
   d) Uveďte adresu IP a masku podsítě pro přepínač *vSwitch1* v sekci **Nastavení připojení pomocí protokolu IP IPVMkernel**.

      Neměňte hodnoty **Maska podsítě** nebo **Výchozí brána VMkernel**.
   e) Uveďte port jádra pro fungování sítě iSCSI.
3. Nastavte virtuální přepínač pro síť virtuálních počítačů.

   Tyto kroky používají pro virtuální přepínač *vSwitch0*.
   a) Vyberte volbu **Virtuální počítač** pro **Typ připojení**.

b) Vyberte volbu **Vytvořit standardní přepínač vSphere** pro **Síťový přístup VMkernel**.

c) Přejděte na kartu **Vlastnosti skupiny portů** a vyberte volbu **Popisek sítě**.

Uveďte stejný štítek, který jste uvedli pro síť virtuálních počítačů *vSwitch1*.

Například: *VMkernel iSCSI*.

4. Svažte nově vytvořený adaptér iSCSI s parametrem **VMkernel Network Adapter**.

Postupujte podle pokynů v proceduře VMware “Svažte adaptéry iSCSI s adaptéry VMkernel”. V době publikace byla tato procedura k dispozici v sekci Dokumentace k produktu VMware ESXi a vCenter Server 5.

Tip: Pokud dojde k uplynutí časového limitu při skenování zařízení iSCSI, snižte počet zařízení iSCSI, která jsou připojena k hostiteli ESXi. Poté zařízení iSCSI procházejte znovu.

5. Ověřte, že jsou vlastnosti svázání adaptéru iSCSI správné.

a) Přejděte do nabídky **Hardware** > **Adaptéry úložiště** v klientovi VMware vSphere.

b) Klepněte pravým tlačítkem myši na adaptér iSCSI a vyberte volbu **Vlastnosti iniciátoru iSCSI**. Ujistěte se, že existují následující vlastnosti vazby:

Tabulka 10. Nastavení sítě iSCSI

Síť virtuálního počítače	Síť iSCSI
Standardní přepínač: *vSwitch0*	**Standardní přepínač**: *vSwitch1*
Skupina portů virtuálního počítače: *Síť virtuálního počítače*	**Port VMkernel**: *VMkernel iSCSI* **Tip:** *VMkernel iSCSI* je svázán s**Adaptérem VMkernel**: *vmk1*, který se nachází na **adaptéru fyzické sítě**: *vmnic1*.
Fyzický adaptér: *vmnic0*	**Síťový adaptér VMkernel**: *vmk1*
	Fyzický síťový adaptér: *vmnic1*
	Virtuální síťový adaptér **adresa IP**: 192.168.42.x (podsíť pro síť iSCSI)

Výsledky

Vyhrazená síť iSCSI je připravena pro úplnou okamžitou obnovu virtuálního počítače a operace okamžitého přístupu.

Konfigurace nastavení zabezpečení produktu Data Protection for VMware

Moduly pro přesouvání dat produktu Data Protection for VMware, rozhraní příkazového řádku vmcli a komponenty grafického rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere vyžadují konfiguraci, která povolí zabezpečené připojení k serveru Server IBM Spectrum Protect.

Konfigurace nastavení zabezpečení pro připojení uzlů modulu pro přesouvání dat a VMCLI k produktu Server IBM Spectrum Protect

Existuje několik voleb konfigurace, které se týkají nastavení zabezpečení produktu Data Protection for VMware pro modul pro přesouvání dat a uzly VMCLI při připojení k produktu Server IBM Spectrum Protect verze V7.1.8 nebo V8.1.2 nebo novější. Přijetí výchozích hodnot pro tyto volby transparentně nakonfiguruje tyto komponenty pro rozšířené zabezpečení a doporučuje se ve většině případů použití.

Konfigurace pomocí výchozích nastavení zabezpečení (rychlý způsob)

Rychlý způsob uvádí podrobnosti voleb konfigurace, které ovlivňují modul pro přesouvání dat a připojení uzlu VMCLI k serveru a chování pro různé případy použití, pokud jsou přijaty výchozí hodnoty. Scénář rychlého způsobu minimalizuje kroky v konfiguračním procesu v koncových bodech.

Tento scénář automaticky získá certifikáty ze serveru, když se uzel poprvé připojí, za předpokladu, že je parametr Server IBM Spectrum Protect **SESSIONSECURITY** nastaven na hodnotu **TRANSITIONAL**, což je výchozí hodnota pro první připojení. Můžete postupovat podle tohoto scénáře, bez ohledu na to, zda nejprve upgradujete server Server IBM Spectrum Protect na verzi V7.1.8 a novější úrovně V7, nebo V8.1.2 a novější úrovně V8, a poté upgradujete produkt Data Protection for VMware, nebo naopak.

Upozornění: Tento scénář nelze použít, pokud je server IBM Spectrum Protect nakonfigurován pro ověření LDAP. Jestliže se používá protokol LDAP, můžete ručně naimportovat nezbytné certifikáty pomocí obslužného programu dsmcert. Podrobnější informace viz “Konfigurace bez automatické distribuce certifikátu” na stránce 58.

Volby uzlu modulu pro přesouvání dat, které ovlivňují zabezpečení relace

Následující volby dsmc uvádí nastavení zabezpečení pro uzel modulu pro přesouvání dat. Další informace o těchto volbách viz Odkaz na volby klienta.

- SSLREQUIRED. Výchozí hodnota Default povoluje existující připojení zabezpečení relace k serverům starším než V7.1.8 nebo V8.1.2 a automaticky konfiguruje modul pro přesouvání dat produktu Data Protection for VMware pro bezpečné připojení k serveru verze V7.1.8 nebo V8.1.2 nebo novější pomocí protokolu TLS pro ověření.
- SSLACCEPTCERTFROMSERV. Výchozí hodnota Yes umožňuje, aby modul pro přesouvání dat ze serveru automaticky přijal veřejný certifikát podepsaný svým držitelem a automaticky nakonfiguroval modul pro přesouvání dat tak, aby použil tento certifikát, když se modul pro přesouvání dat připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější.
- SSL. Výchozí hodnota No označuje, že se nepoužije šifrování při přenosu dat mezi modulem pro přesouvání dat a serverem starším než V7.1.8 nebo V8.1.2. Když se modul pro přesouvání dat připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější, výchozí hodnota No označuje, že data objektu nejsou zašifrovaná. Všechny ostatní informace jsou zašifrované, když modul pro přesouvání dat komunikuje se serverem. Hodnota Yes označuje, že protokol TLS se používá k zašifrování všech informací, včetně dat objektu, když modul pro přesouvání dat komunikuje se serverem.
- SSLFIPSMODE. Výchozí hodnota No označuje, že certifikovaná knihovna TLS standardu FIPS není vyžadována.

Kromě toho následující volby platí jen tehdy, když modul pro přesouvání dat využívá připojení protokolu TLS k serveru ve verzi starší než V7.1.8 nebo V8.1.2. Jsou ignorovány, pokud se modul pro přesouvání dat připojí k novějšímu serveru.

- SSLDISABLELEGACYTLS. Hodnota No označuje, že modul pro přesouvání dat nepožaduje protokol TLS 1.2 pro relace SSL. Umožňuje připojení přes protokol TLS 1.1 a nižší protokoly SSL. Když modul pro přesouvání dat komunikuje se serverem Server IBM Spectrum Protect, který je ve verzi V7.1.7 nebo V8.1.1 nebo starší, volba No je výchozí.
- LANFREESSL. Výchozí hodnota No označuje, že modul pro přesouvání dat nepoužívá protokol TLS ke komunikaci s agentem úložiště, když je konfigurovaný přenos dat bez sítě LAN.
- REPLSSLPORT. Uvádí adresu portu TCP/IP, která je povolena pro protokol TLS, komunikuje-li modul pro přesouvání dat s replikačním cílovým serverem.

Volby uzlu VMCLI, které ovlivňují zabezpečení relace

Následující parametry uvádí nastavení zabezpečení pro uzel VMCLI. Další informace o těchto volbách viz téma Parametry profilu..

- VE_TSM_SSL. Výchozí hodnota NO označuje, že se nepoužije šifrování při přenosu dat mezi modulem pro přesouvání dat a serverem starším než V7.1.8 nebo V8.1.2. Tuto hodnotu nastavte na YES, pokud chcete použít protokol TLS k zašifrování všech informací při připojení k serveru staršímu než V7.1.8.
- VE_TSM_SSLACCEPTCERTFROMSERV. Výchozí hodnota YES umožňuje rozhraní ze serveru automaticky přijmout veřejný certifikát podepsaný svým držitelem a automaticky nakonfigurovat rozhraní tak, aby tento certifikát použilo, když se modul pro přesouvání dat připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější.

- VE_TSM_SSLREQUIRED. Výchozí hodnota DEFAULT povoluje existující připojení zabezpečení relace k serverům starším než V7.1.8 nebo V8.1.2 a automaticky konfiguruje rozhraní pro zabezpečené připojení k serveru verze V7.1.8 nebo V8.1.2 nebo novější pomocí protokolu TLS pro ověření.

Příklady použití pro výchozí nastavení zabezpečení

- Nejprve je server upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější. Poté je upgradován produkt Data Protection for VMware. Existující uzly modulu pro přesouvání dat a VMCLI *nepoužívají* komunikace SSL:
  - Volby zabezpečení pro uzly modulu pro přesouvání dat a VMCLI nevyžadují žádné změny
  - Konfigurace je automaticky aktualizována pro použití protokolu TLS při ověření uzlů na serveru.
- Nejprve je server upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější. Poté je upgradován produkt Data Protection for VMware. Existující uzly modulu pro přesouvání dat a VMCLI *využívají* komunikace SSL:
  - Volby zabezpečení pro uzly modulu pro přesouvání dat a VMCLI nevyžadují žádné změny
  - Komunikace SSL s existujícím veřejným certifikátem serveru se bude nadále používat.
  - Komunikace SSL se automaticky rozšíří tak, že bude používat úroveň protokolu TLS, který vyžaduje server.
- Nejprve je server Data Protection for VMware upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější. Poté je server upgradován později. Existující uzly modulu pro přesouvání dat a VMCLI *nepoužívají* komunikace SSL:
  - Volby zabezpečení pro uzly modulu pro přesouvání dat a VMCLI nevyžadují žádné změny
  - Existující ověřovací protokol je i nadále používán pro servery na úrovních starších než V7.1.8 nebo V8.1.2.
  - Konfigurace je automaticky aktualizována pro použití protokolu TLS při ověření uzlů na serveru, jakmile je aktualizován na verzi V7.1.8 nebo V8.1.2 nebo novější.
- Nejprve je server Data Protection for VMware upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější. Poté je server upgradován později. Existující uzly modulu pro přesouvání dat a VMCLI *využívají* komunikace SSL:
  - Volby zabezpečení pro uzly modulu pro přesouvání dat a VMCLI nevyžadují žádné změny
  - Komunikace SSL s existujícím veřejným certifikátem serveru se bude nadále používat se servery na úrovních starších než V7.1.8 nebo V8.1.2.
  - Komunikace SSL se automaticky rozšíří tak, že bude používat úroveň protokolu TLS, který vyžaduje server po své aktualizaci na verzi V7.1.8 nebo V8.1.2 nebo novější.
- Nejprve je server Data Protection for VMware upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější. Poté se uzly modulu pro přesouvání dat a VMCLI připojí k několika serverům. Servery se upgradují v různých časech:
  - Volby zabezpečení pro uzly modulu pro přesouvání dat a VMCLI nevyžadují žádné změny
  - Uzly modulu pro přesouvání dat a VMCLI používají existující ověření a protokol zabezpečení relací pro servery na verzích starších než V7.1.8 nebo V8.1.2 a automaticky se upgradují pro použití ověření protokolu TLS, když se na začátku připojí k serveru na verzi V7.1.8 nebo V8.1.2 nebo novější. Zabezpečení relace je spravováno pro každý server.
- Nová instalace klienta, server je na verzi V7.1.8 nebo V8.1.2 nebo novější:
  - Nakonfigurujte produkt Data Protection for VMware podle nové instalace.
  - Výchozí hodnoty pro volby zabezpečení automaticky konfigurují uzly modulu pro přesouvání dat a VMCLI pro ověření relace šifrované pomocí protokolu TLS.
  - Nastavte parametr SSL na hodnotu Yes, pokud je šifrování všech přenosů dat mezi klientem a serverem povinné.
- Nová instalace klienta, server je na verzi starší než V7.1.8 nebo V8.1.2:

- Nakonfigurujte klienta podle nové instalace klienta.
- Přijměte výchozí hodnoty pro parametry zabezpečení relace klienta, pokud není šifrování SSL všech přenosů dat povinné.
  - Dokud nebude server upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější, bude se používat protokol bez zabezpečení SSL.
- Nastavte parametr SSL na hodnotu Yes, pokud je povinné šifrování všech přenosů dat mezi modulem pro přesouvání dat a serverem, a pokračujte ruční konfigurací zabezpečení SSL.
  - Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.
  - Komunikace SSL se automaticky rozšíří tak, že bude používat úroveň protokolu TLS, který vyžaduje server po své aktualizaci na verzi V7.1.8 nebo V8.1.2 nebo novější.

Konfigurace bez automatické distribuce certifikátu
Tento scénář podrobně popisuje volby konfigurace, které ovlivňují bezpečnost uzlů modulu pro přesouvání dat a VMCLI, pokud není automatická distribuce certifikátů ze serveru přijatelná. Například automatická distribuce certifikátů ze serveru není přijatelná, pokud je server nakonfigurován tak, aby používal ověření LDAP, nebo je nezbytné, aby byly certifikáty podepsány certifikační autoritou (CA).

Volby, které ovlivňují zabezpečení relace

Volby nastavení zabezpečení jsou stejné jako volby popsané v části “Konfigurace pomocí výchozích nastavení zabezpečení (rychlý způsob)” na stránce 55, jen s výjimkou, že musíte nastavit volbu SSLACCEPTCERTFROMSERV na hodnotu No, abyste zajistili, že uzel modulu pro přesouvání dat automaticky nepřijme veřejný certifikát podepsaný svým držitelem od serveru, když se uzel poprvé připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější.

Příklady použití pro konfiguraci uzlů modulu pro přesouvání dat bez automatické distribuce certifikátů

Jestliže automatická distribuce certifikátů není možná nebo žádoucí, použijte k importu certifikátu obslužný program dsmcert. Nezbytný certifikát získejte ze serveru Server IBM Spectrum Protect nebo od CA. CA může být ze společnosti, jako je VeriSign nebo Thawte, nebo interní CA, která je udržovaná ve vaší společnosti.

Pokud jsou uzly modulu pro přesouvání dat a VMCLI na stejném počítači, požaduje se pouze jeden certifikát. Pokud jsou uzly na oddělených počítačích, certifikát je požadován na každém z nich.

- Nejprve je server upgradován na verzi V7.1.8 nebo V8.1.2. Poté je upgradován produkt Data Protection for VMware. Existující uzly modulu pro přesouvání dat *nepoužívají* komunikace SSL:
  - Nastavte volbu SSLACCEPTCERTFROMSERV pomocí hodnoty No.
  - Získejte nezbytný certifikát ze serveru Server IBM Spectrum Protect nebo od CA a použijte obslužný program dsmcert k importu certifikátu. Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.
- Nejprve je server upgradován na verzi V7.1.8 nebo V8.1.2. Poté je upgradován produkt Data Protection for VMware. Existující uzly modulu pro přesouvání dat *používají* komunikace SSL:
  - Volby zabezpečení pro modul pro přesouvání dat nevyžadují žádné změny Pokud již uzly mají certifikát serveru pro komunikaci SSL, volba SSLACCEPTCERTFROMSERV není platná.
  - Komunikace SSL s existujícím veřejným certifikátem serveru se bude nadále používat.
  - Komunikace SSL se automaticky rozšíří tak, že bude používat úroveň protokolu TLS, který vyžaduje server.
- Nejprve je server Data Protection for VMware upgradován na verzi V7.1.8 nebo V8.1.2. Poté je server upgradován později. Existující uzly modulu pro přesouvání dat *nepoužívají* komunikace SSL:
  - Nastavte volbu SSLACCEPTCERTFROMSERV pomocí hodnoty No.

  - Existující ověřovací protokol je i nadále používán pro servery na úrovních starších než V7.1.8 nebo V8.1.2.
  - Než se uzly modulu pro přesouvání dat připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější:
    - Získejte nezbytný certifikát ze serveru Server IBM Spectrum Protect nebo od CA a použijte obslužný program dsmcert k importu certifikátu. Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.
- Nejprve je server Data Protection for VMware upgradován na verzi V7.1.8 nebo V8.1.2. Poté je server upgradován později. Existující uzly modulu pro přesouvání dat *používají* komunikace SSL.
  - Volby zabezpečení pro modul pro přesouvání dat nevyžadují žádné změny Pokud již uzly mají certifikát serveru pro komunikaci SSL, volba SSLACCEPTCERTFROMSERV není platná.
  - Komunikace SSL s existujícím veřejným certifikátem serveru se bude nadále používat se servery na úrovních starších než V7.1.8 nebo V8.1.2.
  - Komunikace SSL se automaticky rozšíří tak, že bude používat úroveň protokolu TLS, který vyžaduje server po své aktualizaci na verzi V7.1.8 nebo V8.1.2 nebo novější.
- Nejprve je server Data Protection for VMware upgradován na verzi V7.1.8 nebo V8.1.2. Poté se uzly modulu pro přesouvání dat připojí k několika serverům. Servery se upgradují v různých časech:
  - Nastavte volbu SSLACCEPTCERTFROMSERV pomocí hodnoty No.
  - Existující ověřovací protokol je i nadále používán pro servery na úrovních starších než V7.1.8 nebo V8.1.2.
  - Než se uzly modulu pro přesouvání dat připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější nebo pokud je požadována komunikace SSL na libovolné úrovni serveru:
    - Získejte nezbytný certifikát ze serveru Server IBM Spectrum Protect nebo od CA a použijte obslužný program dsmcert k importu certifikátu. Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.
  - Uzly modulu pro přesouvání dat používají existující ověření a protokol zabezpečení relací pro servery na verzích starších než V7.1.8 nebo V8.1.2 a automaticky se upgradují pro použití ověření protokolu TLS, když se na začátku připojí k serveru na verzi V7.1.8 nebo V8.1.2 nebo novější. Zabezpečení relace je spravováno pro každý server.
- Nová instalace produktu Data Protection for VMware, server je na verzi V7.1.8 nebo V8.1.2 nebo novější:
  - Nakonfigurujte produkt Data Protection for VMware podle nové instalace.
  - Nastavte volbu SSLACCEPTCERTFROMSERV pomocí hodnoty No.
  - Získejte nezbytný certifikát ze serveru Server IBM Spectrum Protect nebo od CA a použijte obslužný program dsmcert k importu certifikátu. Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.
  - Nastavte parametr SSL na hodnotu Yes, pokud je šifrování všech přenosů dat mezi modulem pro přesouvání dat a serverem povinné.
- Nová instalace produktu Data Protection for VMware, server je na starší verzi než V7.1.8 nebo V8.1.2, relace šifrované pomocí SSL *jsou* povinné:
  - Nakonfigurujte produkt Data Protection for VMware podle nové instalace.
  - Nastavte parametr SSL na hodnotu Yes.
  - Získejte nezbytný certifikát ze serveru Server IBM Spectrum Protect nebo od CA a použijte obslužný program dsmcert k importu certifikátu. Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.
- Nová instalace produktu Data Protection for VMware, server je na starší verzi než V7.1.8 nebo V8.1.2, relace šifrované pomocí SSL *nejsou* povinné:
  - Nakonfigurujte produkt Data Protection for VMware podle nové instalace.
  - Nastavte volbu SSLACCEPTCERTFROMSERV pomocí hodnoty No.

- Dokud nebude server upgradován na verzi V7.1.8 nebo V8.1.2 nebo novější, bude se používat protokol bez zabezpečení SSL.

– Než se uzly modulu pro přesouvání dat připojí k serveru verze V7.1.8 nebo V8.1.2 nebo novější:

  - Získejte nezbytný certifikát ze serveru Server IBM Spectrum Protect nebo od CA a použijte obslužný program dsmcert k importu certifikátu. Pokyny ke konfiguraci viz téma Konfigurace komunikace klienta/serveru Tivoli Storage Manager se zabezpečením SSL.

Konfigurace komunikace grafického rozhraní produktu Data Protection for VMware vSphere pomocí protokolu TLS

Grafické rozhraní produktu Data Protection for VMware vSphere využívá protokol TLS, čímž poskytuje zabezpečenou komunikaci s webovými prohlížeči; serverem VMware vCenter a volitelně také se serverem Server IBM Spectrum Protect.

Informace o této úloze

Pro komunikaci s webovými prohlížeči a serverem VMware VCenter je protokol TLS vždy povolen. Během instalace produktu Data Protection for VMware je vygenerován digitální certifikát TLS podepsaný svým držitelem a poté je použit pro připojení.

Ke komunikaci s webovými prohlížeči můžete také použít certifikát, který je podepsán certifikační autoritou (CA). Data Protection for VMware Chcete-li použít certifikát od CA, prohlédněte si sekci Použití certifikátu třetí strany pro relace webového prohlížeče.

Pro komunikaci se serverem Server IBM Spectrum Protect použití protokolu TLS závisí na verzi serveru.

Pokud používáte server Server IBM Spectrum Protect verze V7.1.7 nebo V8.1.1 nebo starší
Použití protokolu TLS pro komunikaci se serverem je volitelné. Můžete ručně povolit grafické rozhraní produktu Data Protection for VMware vSphere pro komunikaci se serverem přes protokol TLS vytvořením nebo aktualizací úložiště údajů o důvěryhodnosti a importem certifikátu podle popisu v sekci “Povolení zabezpečené komunikace se serverem IBM Spectrum Protect” na stránce 60

Pokud používáte server Server IBM Spectrum Protect verze 7.1.8 nebo V8.1.2 nebo novější
Protokol TLS je povinný. Ve většině případů se úložiště údajů o důvěryhodnosti vytvoří automaticky při prvním použitím pomocí výchozích nastavení zabezpečení popsaných v sekci “Konfigurace pomocí výchozích nastavení zabezpečení (rychlý způsob)” na stránce 55. Nicméně v některých scénářích budete možná muset úložiště údajů o důvěryhodnosti vytvořit ručně. .

Důležité: Scénář rychlého způsobu automaticky získá certifikáty, když grafické rozhraní produktu Data Protection for VMware vSphere poprvé komunikuje se serverem, za předpokladu, že je parametr Server IBM Spectrum Protect **SESSIONSECURITY** nastaven na hodnotu **TRANSITIONAL**, což je výchozí hodnota pro první připojení. Poté, co se grafické rozhraní připojí k serveru, parametr **SESSIONSECURITY** je nastaven na hodnotu **STRICT**. Protože grafické rozhraní využívá ID administrátora serveru pro připojení k serveru, použije-li jiná entita toto ID pro připojení, zobrazí se při pokusu o připojení k serveru v grafickém rozhraní chybová zpráva. Chcete-li vyřešit tento problém, nastavte parametr **SESSIONSECURITY** zpět na hodnotu **TRANSITIONAL**.

Povolení zabezpečené komunikace se serverem IBM Spectrum Protect

Pokud používáte server IBM Spectrum Protect verze V7.1.7 nebo starší, nebo V8.1.2 nebo starší, připojení k serveru pomocí protokolu TLS je volitelné, a chcete-li povolit komunikaci grafického rozhraní produktu Data Protection for VMware vSphere se serverem pomocí protokolu, musíte tuto komunikaci povolit ručně.

Než začnete

Získejte kopii certifikátu od administrátora serveru.

Informace o této úloze

Pokud používáte server verze V7.1.8 nebo V8.1.2 nebo novější, protokol TLS je vyžadován a úložiště údajů o důvěryhodnosti s certifikátem se vytvoří automaticky při prvním použití pomocí výchozích nastavení

zabezpečení, které jsou popsány v části “Konfigurace pomocí výchozích nastavení zabezpečení (rychlý způsob)” na stránce 55. Nicméně v některých scénářích budete možná muset ručně vytvořit úložiště údajů o důvěryhodnosti a konfigurovat grafické rozhraní produktu Data Protection for VMware vSphere, jak je popsáno v tomto tématu.

Následující procedura používá klíč Java™ a nástroj pro správu certifikátů **keytool**.

Na operačních systémech Linux se nástroj nachází v adresáři `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Na operačních systémech Microsoft Windows je nástroj umístěný v adresáři `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre\bin`.

Při spouštění příkazu **keytool** budete nejspíš muset uvést úplnou cestu.

Postup

1. Z příkazového řádku změňte adresář na umístění úložiště údajů o důvěryhodnosti:
   - na systému Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`
   - Windows: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\`
2. Vytvořte úložiště údajů o důvěryhodnosti a naimportujte certifikát tímto příkazem:

   ```
   keytool -importcert -alias my-cert -file cert.pem -keystore
   tsm-ve-truststore.jks -storepass password
   ```

   Kde:

   -alias *my-cert*
   Jedinečný alias, který identifikuje certifikát v úložišti údajů o důvěryhodnosti.

   -file *cert.pem*
   Soubor, který obsahuje certifikát serveru podepsaný držitelem nebo kořenový certifikát CA.

   -storepass *password*
   Heslo úložiště klíčů. Zajistěte, abyste si heslo zapamatovali pro budoucí použití.
3. Spusťte grafické rozhraní produktu Data Protection for VMware vSphere a přejděte do okna **Konfigurace**.
   - Pokud vytváříte počáteční konfiguraci, klepněte na nabídku **Úlohy** > **Spustit průvodce konfigurací produktu IBM Spectrum Protect** a přejděte na stránku **Pověření serveru**.
   - Pokud upravujete existující konfiguraci, klepněte na nabídku **Úlohy** > **Upravit konfiguraci produktu IBM Spectrum Protect** a přejděte na stránku **Pověření serveru**.
4. Do pole **Port administrátora produktu IBM Spectrum Protect** zadejte číslo portu. Jedná se o port serveru, který umožňuje administrativní připojení pomocí protokolu SSL nebo TLS.
5. Vyberte volbu **Použít šifrovanou komunikaci na portu administrátora**.
6. Chcete-li použít toto nastavení pro budoucí relace grafického rozhraní, vyberte volbu **Uložit ID administrátora, heslo a nastavení portu**.
7. Klepněte na tlačítko **OK**, abyste uložili změny.

Použití certifikátu od certifikační autority

Chcete-li použít certifikát, který je podepsán certifikační autoritou (CA), musíte provést několik kroků.

Informace o této úloze

Následující procedury používají standardní nástroj pro správu klíčů a certifikátu nazvaný **keytool**.

Na operačních systémech Linux je umístěn v adresáři `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Na operačních systémech Microsoft Windows je umístěn v adresáři `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre`.

Při spuštění nástroje **keytool** z příkazového řádku budete zřejmě uvádět úplnou cestu.

Postup

1. Získejte přístup k úložišti klíčů.
2. Vytvořte požadavek na podpis certifikátu (CSR).
3. Odešlete požadavek na podpis certifikátu certifikační autoritě k podepsání.
4. Přijměte podepsaný certifikát do grafického rozhraní produktu Data Protection for VMware vSphere.

Získání přístupu k úložišti klíčů

Certifikáty se ukládají do úložiště klíčů Java. Obsah úložiště klíčů je chráněn heslem. Chcete-li manipulovat s certifikáty v úložišti klíčů, musíte k němu získat přístup.

Informace o této úloze

Výchozí certifikát podepsaný svým držitelem a heslo úložiště klíčů jsou automaticky generovány během instalace, takže pravděpodobně nebudete znát počáteční heslo.

Dokončením této procedury nahradíte původní úložiště klíčů novým úložištěm klíčů a novým certifikátem podepsaným svým držitelem. Nové úložiště klíčů je chráněno heslem dle vlastního výběru.

Pokud již znáte heslo úložiště klíčů, přeskočte tento postup.

Postup

1. Zastavte službu grafického rozhraní produktu Data Protection for VMware vSphere.
2. V příkazovém řádku změňte adresář na umístění úložiště klíčů.
   - Pro operační systém Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Pro operační systém Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
3. Vytvořte záložní kopii souboru úložiště klíčů (`key.jks`) jeho přejmenováním nebo přesunutím do jiného umístění.
4. Vytvořte nové úložiště klíčů a nový certifikát podepsaný svým držitelem zadáním tohoto příkazu:

```
keytool -genkeypair -alias vekey -dname
CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
-sigalg SHA256withRSA -keysize 2048 -validity days -keystore
key.jks -storepass password -keypass password
```

   Kde:

   -dname CN=*fqdn*,OU=Tivoli_Storage_Manager_for_VMware,O=IBM
   fqdn je název serveru názvů domény nebo úplný název domény počítače, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere.

   -validity *days*
   Období platnosti certifikátu.

   -storepass *password*
   Heslo úložiště klíčů. Zajistěte, abyste si heslo zapamatovali pro budoucí použití.

   -keypass *password*
   Heslo soukromého klíče pro certifikát. Toto heslo musí odpovídat heslu úložiště klíčů.
5. Zakódujte heslo úložiště klíčů pomocí nástroje **securityUtility**. Spusťte následující příkaz.
   - Pro operační systém Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - Pro operační systém Windows: `C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode`

Na vyžádání zadejte heslo úložiště klíčů a poté uložte výstup (například jej zkopírujte do schránky).

6. Otevřete soubor `bootstrap.properties` v editoru a nastavte vlastnost `veProfile.keystore.pswd` na zakódovanou hodnotu z předchozího kroku.

   Soubor `bootstrap.properties` je v následujícím umístění:

   - Pro operační systém Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
   - Pro operační systém Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\`
7. Spusťte službu grafického rozhraní produktu Data Protection for VMware vSphere.

Související odkazy

“Spuštění a provoz služeb produktu Data Protection for VMware” na stránce 80
Standardně se při spuštění operačního systému Windows spustí agent zotavení pod účtem lokálního systému.

Vytváření požadavku na podpis certifikátu

Po obdržení přístupu do úložiště klíčů musíte vytvořit požadavek na podpis certifikátu (CSR).

Postup

Tímto postupem vytvoříte požadavek na podpis certifikátu:

1. V příkazovém řádku změňte adresář na umístění úložiště klíčů.
   - Pro operační systém Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Pro operační systém Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Vytvořte nový certifikát zadáním tohoto příkazu:

   ```
   keytool -genkeypair -alias mykey -dname
   CN=fqdn,OU=jednotka,O=organizace -keyalg RSA -sigalg SHA256withRSA
   -keysize 2048 -validity dny -keystore key.jks -storepass
   heslo -keypass heslo
   ```

   Kde:

   -alias *mykey*
   mykey je jedinečný alias, který identifikuje certifikát v úložišti klíčů. Přejmenuje se při přijetí podepsaného certifikátu.

   -dname CN=*fqdn*,OU=*jednotka*,O=*organizace*
   fqdn je název serveru názvů domény nebo úplný název domény počítače, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere.

   Jednotka a *organizace* jsou informace o organizaci, které vyžadují vaše zásady nebo certifikační autorita.

   -validity *days*
   Období platnosti certifikátu.

   -storepass *password*
   Heslo úložiště klíčů. Pokud neznáte nebo jste zapomněli heslo úložiště klíčů, prohlédněte si sekci “Získání přístupu k úložišti klíčů” na stránce 62.

   -keypass *password*
   Heslo soukromého klíče pro certifikát. Toto heslo musí odpovídat heslu úložiště klíčů.
3. Vytvořte požadavek na podpis certifikátu zadáním tohoto příkazu:

   ```
   keytool -certreq -alias mykey -file certreq.pem -keystore key.jks
   ```

   Kde:

-alias *mykey*
Alias certifikátu z předchozího kroku.

-file *certreq.pem*
Soubor pro uložení požadavku na podpis certifikátu.

Odeslání požadavku na podepsání certifikátu certifikační autoritě

Po vytvoření žádosti o certifikát (`certreq.pem`) jej musíte odeslat certifikační autoritě k podpisu. Postupujte podle specifických instrukcí od certifikační autority.

Přijetí podepsaných certifikátů

Jakmile obdržíte podepsaný certifikát od certifikační autority (CA), musíte jej přijmout do úložiště klíčů.

Postup

Chcete-li přijmout podepsaný certifikát, postupujte takto:

1. V příkazovém řádku změňte adresář na umístění úložiště klíčů.
   - Pro operační systém Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Pro operační systém Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Zkopírujte soubory, které jste přijali od certifikační autority, do tohoto umístění. Tyto soubory zahrnují kořenový certifikát certifikační autority, přechodné certifikáty certifikační autority (pokud existuje) a podepsaný certifikát pro grafické rozhraní produktu Data Protection for VMware vSphere.
3. Zastavte službu grafického rozhraní produktu Data Protection for VMware vSphere.
4. Vytvořte záložní kopii souboru úložiště klíčů (`key.jks`) jeho zkopírováním do jiného názvu nebo umístění.
5. Importujte přechodné certifikáty certifikační autority, pokud takové existují, pomocí následujícího příkazu. Na výzvu důvěřovat certifikátům odpovězte *yes*. Tento krok zopakujte pro všechny přechodné certifikáty certifikační autority dle potřeby.

   ```
   keytool -importcert -alias ca-intermediate -file intermediate.pem
   -keystore key.jks -storepass heslo
   ```

   Kde:

   -alias *ca-intermediate*
   Jedinečný alias, který identifikuje certifikát v úložišti klíčů. Každý přechodný certifikát musí mít jedinečný alias.

   -file *intermediate.pem*
   Soubor přechodného certifikátu, který je získán od certifikační autority.

   -storepass *password*
   Heslo úložiště klíčů.
6. Importujte kořenový certifikát certifikační autority zadáním následujícího příkazu. Na výzvu důvěřovat tomuto certifikátu odpovězte *yes*.

   ```
   keytool -importcert -alias ca-root -file root.pem -keystore
   key.jks -storepass heslo
   ```

   Kde:

   -alias *ca-root*
   Jedinečný alias, který identifikuje certifikát v úložišti klíčů.

   -file *root.pem*
   Soubor kořenového certifikátu získaného od certifikační autority.

   -storepass *password*
   Heslo úložiště klíčů.
7. Importujte podepsaný certifikát zadáním následujícího příkazu:

```
keytool -importcert -alias mykey -file signedcert.pem -keystore
key.jks -storepass heslo
```

Kde:

-alias *mykey*
Alias pro podepsaný certifikát. Alias musí být stejné jako to, které jste použili při vytváření úložiště klíčů. Další podrobnosti o vytváření nového úložiště klíčů a nového certifikátu podepsaného držitelem naleznete v tématu Získání přístupu k úložišti klíčů.

-file *signedcert.pem*
Soubor podepsaného certifikátu přijatý od certifikační autority.

-storepass *password*
Heslo úložiště klíčů.

8. Spusťte službu grafického rozhraní produktu Data Protection for VMware vSphere.

Související odkazy

“Spuštění a provoz služeb produktu Data Protection for VMware” na stránce 80
Standardně se při spuštění operačního systému Windows spustí agent zotavení pod účtem lokálního systému.

Požadavky na oprávnění uživatelů serveru VMware vCenter

Ke spuštění operací produktu Data Protection for VMware jsou zapotřebí jistá oprávnění serveru VMware vCenter.

Oprávnění serveru vCenter požadovaná k ochraně datových středisek VMware s pohledem webového prohlížeče pro grafické rozhraní produktu Data Protection for VMware vSphere

ID uživatele serveru vCenter Server, který se přihlásí do zobrazení prohlížeče, pro grafické rozhraní produktu Data Protection for VMware vSphere

musí mít dostateční oprávnění VMware k zobrazení obsahu datového střediska spravovaného grafickým rozhraním.

Prostředí VMware vSphere například obsahuje pět datových středisek. Uživatel, "jenn", má dostatečná oprávnění pouze pro dvě z těchto datových středisek. V důsledku toho jsou pouze tato dvě datová střediska, kde existují dostatečná oprávnění, pro uživatele "jenn" viditelná v pohledech. Ostatní tři datová střediska (kde uživatel "jenn" nemá oprávnění) nejsou pro tohoto uživatele viditelná.

Server VMware vCenter definuje sadu oprávnění společně jako roli. Role se použije na objekt pro určeného uživatele nebo určenou skupinu pro vytvoření oprávnění. Z webového klienta VMware vSphere musíte vytvořit roli se sadou oprávnění. Chcete-li vytvořit roli serveru vCenter pro operace zálohy a obnovy, použijte funkci klienta VMware vSphere **Přidat roli**.

Chcete-li šířit oprávnění na všechna datová střediska v produktu vCenter, uveďte server vCenter a zaškrtněte zaškrtávací políčko `Šířit na podřízené prvky`. Jinak můžete omezit oprávnění, přiřadíte-li roli k požadovaným datovým střediskům výhradně se zaškrtnutým zaškrtávacím políčkem `Šířit na podřízené prvky`. Vynucení pro grafická rozhraní prohlížeče je na úrovni datového střediska.

Následující příklad ukazuje, jak řídit přístup k datovým střediskům pro dvě skupiny uživatelů VMware. Nejprve vytvořte roli, která obsahuje všechna oprávnění nadefinovaná v technické poznámce 7047438. Sada oprávnění v tomto příkladu je identifikována rolí nazvanou "TDPVMwareManage". Skupina 1 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska `Primary1_DC` a `Primary2_DC`. Skupina 2 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska `Secondary1_DC` a `Secondary2_DC`.

Pro skupinu 1 přiřaďte roli "TDPVMwareManage" k datovým střediskům `Primary1_DC` a `Primary2_DC`. Pro skupinu 2 přiřaďte roli "TDPVMwareManage" k datovým střediskům `Secondary1_DC` a `Secondary2_DC`.

Uživatelé v každé skupině uživatelů VMware mohou použít grafické rozhraní produktu Data Protection for VMware ke správě virtuálních počítačů pouze ve svých odpovídajících datových střediscích.

Tip: Když vytváříte roli, zvažte přidání dalších oprávnění do role, které můžete později potřebovat k dokončení jiných úloh na objektech.

Oprávnění serveru vCenter požadovaná pro použití modulu pro přesouvání dat

Modul pro přesouvání dat IBM Spectrum Protect, který je nainstalován na záložním serveru vStorage (uzel modulu pro přesouvání dat) vyžaduje volby VMCUser a VMCPw. Volba VMCUser uvádí ID uživatele serveru vCenter nebo ESX, který chcete zálohovat, obnovit nebo dotazovat. Požadovaná oprávnění přiřazená k danému ID uživatele (VMCUser) zajistí, že klient může spustit operace na virtuálním počítači a v prostředí VMware. Toto ID uživatele musí mít oprávnění VMware, která jsou popsaná ve výše uvedené technické poznámce.

Chcete-li vytvořit roli serveru vCenter pro operace zálohy a obnovy, použijte funkci klienta VMware vSphere **Přidat roli**. Musíte vybrat volbu Šířit na podřízené položky, přidáváte-li oprávnění pro toto ID uživatele (VMCUser). Kromě toho zvažte přidání dalších oprávnění k této roli pro ostatní úlohy kromě zálohy a obnovy. Pro volbu VMCUser je vynucení objekt nejvyšší úrovně.

Oprávnění serveru vCenter požadovaná k ochraně datových středisek VMware s pohledem modulu IBM Spectrum Protect vSphere Client plug-in pro grafické rozhraní produktu Data Protection for VMware vSphere

Modul IBM Spectrum Protect vSphere Client plug-in vyžaduje sadu oprávnění, která jsou oddělená od oprávnění vyžadovaných pro přihlášení ke grafickému rozhraní.

Během instalace jsou vytvořena následující vlastní oprávnění pro modul IBM Spectrum Protect vSphere Client plug-in:

- **Datové středisko** > **IBM Data Protection**
- **Globální** > **Konfigurovat produkt IBM Data Protection**

Vlastní oprávnění, která jsou požadována pro modul IBM Spectrum Protect vSphere Client plug-in, jsou registrována jako oddělené rozšíření. Klíč rozšíření oprávnění je com.ibm.tsm.tdpvmware.IBMDataProtection.privileges.

Tato oprávnění umožňují administrátorovi VMware povolit a zakázat přístup k obsahu modulu IBM Spectrum Protect vSphere Client plug-in. Pouze uživatelé s těmito vlastními oprávněními na požadovaném objektu VMware mohou získat přístup k obsahu modulu IBM Spectrum Protect vSphere Client plug-in. Jeden modul IBM Spectrum Protect vSphere Client plug-in je registrován pro každý server a je sdílen všemi hostiteli grafického rozhraní, kteří jsou konfigurováni pro podporu serveru vCenter.

Z webového klienta VMware vSphere musíte vytvořit roli pro uživatele, kteří mohou provádět funkce ochrany dat pro virtuální počítače pomocí modulu IBM Spectrum Protect vSphere Client plug-in. Pro tuto roli, kromě standardních oprávnění role administrátora virtuálního počítače požadovaných webovým klientem, musíte uvést oprávnění **Datové středisko** > **IBM Data Protection**. Pro každé datové středisko přiřaďte tuto roli pro každého uživatele nebo skupinu, kde chcete udělit oprávnění, aby uživatel mohl spravovat virtuální počítače.

Oprávnění **Globální** > **IBM Data Protection** je vyžadováno pro uživatele na úrovni produktu vCenter. Toto oprávnění umožňuje uživateli spravovat, upravit nebo vymazat připojení mezi serverem vCenter a webovým serverem grafického rozhraní produktu Data Protection for VMware vSphere. Přiřaďte toto oprávnění k administrátorům, kteří jsou obeznámeni s grafickým rozhraním produktu Data Protection for VMware vSphere chránícím jejich příslušné servery vCenter. Svoje připojení k modulu IBM Spectrum Protect vSphere Client plug-in spravujte na stránce rozšíření **Připojení**.

Následující příklad zobrazuje, jak řídit přístup k datovým střediskům pro dvě skupiny uživatelů. Skupina 1 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska NewYork DC a Boston_DC. Skupina 2 vyžaduje přístup pro správu virtuálních počítačů pro datová střediska LosAngeles_DC a SanFranciso_DC.

Z klienta VMware vSphere vytvořte například roli "IBMDataProtectManage", přiřaďte standardní oprávnění role administrátora virtuálních počítačů a také oprávnění **Datové středisko** > **IBM Data Protection**.

Pro skupinu 1 přiřaďte roli "IBMDataProtectManage" k datovým střediskům `NewYork DC` a `Boston_DC`. Pro skupinu 2 přiřaďte roli "IBMDataProtectManage" k datovým střediskům `LosAngeles_DC` a `SanFranciso_DC`.

Uživatelé v každé skupině mohou používat modul IBM Spectrum Protect vSphere Client plug-in v prostředí webového klienta vSphere ke správě virtuálních počítačů pouze ve svých odpovídajících datových střediscích.

Problémy týkající se nedostatečných oprávnění

Když nemá uživatel webového prohlížeče dostatečná oprávnění k jakémukoli datovému středisku, přístup k pohledu je blokován. Namísto toho se objeví chybová zpráva GVM2013E, která oznamuje, že uživatel není autorizován pro přístup k žádným spravovaným datovým střediskům vzhledem k nedostatečným oprávněním. Jsou rovněž k dispozici další nové zprávy, které informují uživatele o problémech způsobených nedostatečnými oprávněními. Chcete-li vyřešit případné problémy související s oprávněními, ujistěte se, že role uživatele je nastavena tak, jak je popsáno v předchozích sekcích. Role uživatele musí mít všechna oprávnění, která jsou identifikována v tabulce Požadovaných oprávnění ID uživatele serveru vCenter a modulu pro přesouvání dat, a tato oprávnění musí být použita na úrovni datového centra se zaškrtávacím políčkem `Šířit na podřízené prvky`.

Když nemá uživatel modulu IBM Spectrum Protect vSphere Client plug-in dostatečná oprávnění pro datové středisko, funkce ochrany dat pro toto datové středisko a jeho obsah nejsou v rozšíření k dispozici.

Když ID uživatele IBM Spectrum Protect (uvedené volbou `VMCUser`) obsahuje nedostatečná oprávnění pro operace zálohy a obnovy, zobrazí se následující zpráva:

```
ANS9365E Chyba rozhraní API VMware vStorage.
"Oprávnění pro provedení této operace bylo odepřeno."
```

Když ID uživatele IBM Spectrum Protect obsahuje nedostatečná oprávnění pro zobrazení počítače, zobrazí se následující zpráva:

```
Příkaz Backup VM byl spuštěný.
Celkový počet virtuálních počítačů ke zpracování: 1
ANS4155E Virtuální počítač 'tango' nebyl na serveru VMware nalezen.
ANS4148E Úplná záloha virtuálního počítače 'foxtrot' selhala s návratovým kódem 4390
```

Další informace k používání oprávnění najdete v poznámce **Oprávnění serveru vCenter požadovaná pro použití modulu pro přesouvání dat**.

Chcete-li načíst informace o protokolu prostřednictvím serveru VMware Virtual Center a hledat problémy s oprávněním, postupujte takto:

1. V nabídce **Nastavení serveru vCenter** vyberte volbu **Volby protokolování** a nastavte volbu "**Protokolování vCenter** na hodnotu **Trivia (Trivia)**.
2. Znovu vyvolejte chybu oprávnění.
3. Resetujte volbu **Protokolování vCenter** na předchozí hodnotu, což zabraňuje záznamu nadměrného množství informací v protokolu.
4. V nabídce **Systémové protokoly** vyhledejte nejaktuálnější protokol serveru vCenter (`vpxd-`*`wxyz`*`.log`) a vyhledejte řetězec `NoPermission`. Například:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Tato zpráva protokolu označuje, že ID uživatele neobsahovalo dostatečná oprávnění pro vytvoření snímku (`createSnapshot`).

Role uživatelů grafického rozhraní produktu Data Protection for VMware vSphere

Dostupnost funkcí grafického rozhraní produktu Data Protection for VMware vSphere je založena na úrovni oprávnění přiřazené vašemu ID administrátora produktu IBM Spectrum Protect.

ID administrátora musí odpovídat názvu uzlu. Ve starších vydáních produktu příkaz **REGISTER NODE** automaticky vytvořil ID administrativního uživatele, jehož jméno se shodovalo s názvem uzlu. Počínaje verzí produktu IBM Spectrum Protect 8.1 příkaz **REGISTER NODE** automaticky nevytváří ID administrativního uživatele, jehož jméno se shoduje s názvem uzlu.

Při registraci nového uzlu musí administrátor serveru IBM Spectrum Protect zadat v příkazu serveru **REGISTER NODE** parametr `userid`:

```
REGISTER NODE název_uzlu heslo userid=ID_uživatele
```

Kde se název uzlu a ID administrativního uživatele musí shodovat. Například:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

Uzel má standardně oprávnění vlastníka klienta.

Úlohy, které můžete spouštět pomocí grafického rozhraní produktu Data Protection for VMware vSphere, jsou založeny na třídě oprávnění přiřazené k ID administrátora.

Když nemá ID administrátora neomezená oprávnění domény zásad, nemůžete registrovat nové uzly, nebo nastavit jejich vztah serveru proxy na serveru IBM Spectrum Protect. Pokud nezadáte ID administrátora, je vytvořen skript makra, takže můžete provést spuštění na serveru IBM Spectrum Protect.

ID administrátora produktu IBM Spectrum Protect je vyžadováno při konfiguraci grafického rozhraní produktu Data Protection for VMware vSphere. Tato tabulka vypisuje funkce dostupné na základě třídy oprávnění přiřazené k tomuto ID:

- Hodnota Ano označuje dostupnou funkci pro roli uživatele.
- Hodnota ne označuje funkci, která není pro roli uživatele k dispozici.

Chcete-li zobrazit aktuální roli grafického rozhraní produktu Data Protection for VMware vSphere podržte kurzor nad vaším ID uživatele v navigačním panelu.

Tabulka 11. Dostupné funkce založené na požadavcích na oprávnění ID administrátora produktu IBM Spectrum Protect

	Operátor	**Operátor s vytvářením sestav**	**Omezený administrátor**	**Administrátor**
Souhrn	Spustit nyní zálohování a obnovu	Operátor plus vytváření sestav	Operátor plus vytváření sestav a plánované operace pro vypsané domény zásad	Všechny role včetně počáteční konfigurace
ID administrátora IBM Spectrum Protect Třída oprávnění	Žádný	Jedna z následujících tříd oprávnění: • Úložiště • Operátor • Analytik	Zásada (omezená) nebo jedna z následujících tříd oprávnění: • Úložiště • Operátor • Analytik	Zásada (neomezená) nebo systém
Karta Záloha				
Spravovat úlohy zálohování typu **Spustit nyní**	Ano	Ano	Ano	Ano
Spravovat úlohy zálohování typu **Naplánovaná**	Ne[1]	Ne[1]	Ano s doménami zásad	Ano

Tabulka 11. Dostupné funkce založené na požadavcích na oprávnění ID administrátora produktu IBM Spectrum Protect (pokračování)

	Operátor	Operátor s vytvářením sestav	Omezený administrátor	Administrátor
Zobrazit úlohy zálohování typu **Spustit nyní**	Ano	Ano	Ano	Ano
Zobrazit úlohy zálohování typu **Naplánovaná**	Ne	Ano	Ano	Ano
Odstranit úlohy zálohování typu **Naplánovaná**	Ne	Ne	Ano s doménami zásad	Ano
Karta Obnova				
Spustit úlohu **Obnova**	Ano	Ano	Ano	Ano
Karta Sestavy				
události	Ne	Ano	Ano	Ano
poslední úlohy	Ano	Ano	Ano	Ano
stav zálohování	Ne	Ano	Ano	Ano
Ochrana aplikace	Ne	Ano	Ano	Ano
Obsazenost datového střediska	Ne	Ano	Ano	Ano
Karta Konfigurace				
Registrace uzlu (**Stav konfigurace** -> **Spustit průvodce konfigurací**)	Ne	Ne	Ne[2]	Ano
Změnit pověření ID administrátora IBM Spectrum Protect (**Stav konfigurace** -> **Upravit konfiguraci**)	Ano	Ano	Ano	Ano
Změnit heslo uzlu VMCLI (**Stav konfigurace** -> **Upravit konfiguraci**)	Ne	Ne	Ano	Ano
Změnit domény grafického rozhraní (**Stav konfigurace** -> **Upravit konfiguraci**)	Ano[3]	Ano[3]	Ano[3]	Ano
Změnit uzly modulu pro přesouvání dat (**Stav konfigurace** -> **Upravit konfiguraci**)	Ne	Ne	Ne[2]	Ano
Změnit uzly serveru proxy pro připojení (**Stav konfigurace** -> **Upravit konfiguraci**)	Ne	Ne	Ne[2]	Ano

Tabulka 11. Dostupné funkce založené na požadavcích na oprávnění ID administrátora produktu IBM Spectrum Protect (pokračování)

	Operátor	Operátor s vytvářením sestav	Omezený administrátor	Administrátor
1. Nemůžete registrovat uzel, protože je požadována zásada odregistrované domény. 2. Můžete přidat nebo odebrat datová střediska VMware a registrovat uzly datových středisek.				

Chcete-li zobrazit úroveň oprávnění ID administrátora IBM Spectrum Protect a odpovídající role grafického rozhraní produktu Data Protection for VMware vSphere, postupujte takto:

1. Přejděte do okna **Konfigurace**.
2. Klepněte na volbu **Upravit konfiguraci**.
3. Příslušné informace jsou zobrazeny na stránce **Pověření serveru Spectrum Protect Server**.

Důležité:

- Pokud se úroveň oprávnění ID administrátora produktu IBM Spectrum Protect na serveru IBM Spectrum Protect změní, musí být restartováno grafické rozhraní produktu Data Protection for VMware vSphere, aby se tato změna projevila.
- Když změníte **roli uživatele**, musíte klepnout na tlačítko **OK**, abyste uložili změny, než přejdete na další stránku **Nastavení konfigurace** nebo se pokusíte o jinou změnu konfigurace. Jinak se změny **role uživatele** neprojeví.

Registrační klíče grafického uživatelského rozhraní produktu Data Protection for VMware

V závislosti na volbách, které vyberete během instalace, můžete vstoupit do grafického rozhraní produktu Data Protection for VMware pomocí různých metod. Registrační klíče se vytvoří pro grafická uživatelská rozhraní produktu Data Protection for VMware.

Fráze "Grafické rozhraní produktu Data Protection for VMware" se vztahuje na následující grafická rozhraní:

- grafické rozhraní produktu Data Protection for VMware vSphere zpřístupněné ve webovém prohlížeči
- modul IBM Spectrum Protect vSphere Client plug-in v grafickém rozhraní webového klienta vSphere

Registrační klíč modulu IBM Spectrum Protect vSphere Client plug-in je `com.ibm.tsm.tdpvmware.IBMDataProtection`. Tento klíč je registrován při zaškrtnutí zaškrtávacího políčka **Registrovat jako rozšíření webového klienta vSphere** během instalace. Na jeden server vCenter je registrována jediná instance modulu IBM Spectrum Protect vSphere Client plug-in.

Registrační klíč se nevytvoří pro grafické rozhraní produktu Data Protection for VMware vSphere, ke kterému se přistoupí ve webovém prohlížeči.

Chcete-li zobrazit registrační klíče, přihlaste se do prohlížeče spravovaných objektů VMware (MOB). Po přihlášení do prohlížeče spravovaných objektů přejděte do nabídky **Obsah→Správce rozšíření**, kde zobrazíte registrační klíče.

Konfigurace grafického rozhraní agenta zotavení

Jsou poskytnuty instrukce pro nastavení grafického rozhraní agenta zotavení pro operace připojení, obnovy souboru nebo okamžité obnovy.

Než začnete
Tyto konfigurační úlohy musí být dokončeny před pokusem o operaci v grafickém rozhraní agenta zotavení.

Důležité: Informace o tom, jak provádět úlohy pomocí grafického rozhraní agenta zotavení naleznete v nápovědě online, která je nainstalována s grafickým rozhraním. Klepnutím na tlačítko **Nápověda** v jakémkoli okně grafického rozhraní otevřete nápovědu online pro podporu úlohy.

Postup

1. Přihlaste se na systém, kam chcete obnovit soubory. Agent zotavení musí být na systému nainstalován.
2. Klepnutím na volbu **Vybrat server TSM** v grafickém rozhraní agenta zotavení se připojte k serveru IBM Spectrum Protect.

   Když je agent zotavení nainstalovaný na stejném systému jako agent Data Protection for VMware vSphere a aplikace byly úspěšně nakonfigurovány pomocí průvodce konfigurací grafického rozhraní produktu Data Protection for VMware vSphere, pak existují následující kritéria:

   - Server uzel modulu pro přesouvání dat a IBM Spectrum Protect je naplněn daty v poli zotavení **TSM Server**.
   - Následující pole jsou naplněna daty v panelu **Informace o serveru TSM**:
     - **Uzel ověření** obsahuje seznam dostupných uzlů modulů pro přesouvání dat.
     - **Cílový uzel** obsahuje seznam uzlů datového centra, které jsou k dispozici pro zvolený uzel modulu pro přesouvání dat.

   Pokud jste pomocí průvodce konfigurací nakonfigurovali pouze jeden lokální uzel modulu pro přesouvání dat, agent zotavení použije daný uzel k ověření při spuštění.

   Agent zotavení si pamatuje poslední název uzlu připojeného k serveru IBM Spectrum Protect. Pokud je vybrána volba **Použít generování přístupu k heslu** pro tento uzel (poslední název uzlu k připojení), agent zotavení použije tato pověření k připojení k serveru IBM Spectrum Protect při spuštění. Pokud nebylo dokončeno žádné předchozí připojení k serveru IBM Spectrum Protect, nakonfiguruje se průvodcem pouze uzel modulu pro přesouvání dat a uzel datového střediska a agent zotavení použije tato pověření k připojení k serveru IBM Spectrum Protect při spuštění.

   Uveďte následující volby:

   Adresa serveru
   Zadejte adresu IP nebo název hostitele serveru IBM Spectrum Protect.

   Port serveru
   Zadejte číslo portu použité pro komunikaci TCP/IP se serverem. Výchozí číslo portu je 1500.

   Přístupová metoda k uzlu:

   Jako název uzlu
   Vyberte tuto volbu, chcete-li použít uzel serveru proxy pro přístup k zálohám virtuálního počítače v cílovém uzlu. Uzel serveru proxy je uzel, kterému je uděleno oprávnění "proxy" k provedení operací jménem cílového uzlu.

   Obvykle používá administrátor funkce IBM Spectrum Protect příkaz `grant proxynode` k vytvoření vztahu serveru proxy mezi dvěma existujícími uzly.

   Pokud tuto volbu vyberete, postupujte takto:

   a. Zadejte název cílového uzlu (uzel, na kterém jsou místěny zálohy virtuálního počítače) v poli **Cílový uzel**.
   b. Zadejte název uzlu serveru proxy v poli **Uzel ověření**.
   c. Zadejte heslo pro uzel serveru proxy v poli **Heslo**.
   d. Klepnutím na tlačítko **OK** uložte tato nastavení a ukončete dialogové okno informací o funkci IBM Spectrum Protect.

   Když použijete tuto metodu, uživatel agenta zotavení zná pouze heslo uzlu serveru proxy a heslo cílového uzlu je chráněné.

Z uzlu
Vyberte tuto volbu, chcete-li použít uzel s přístupem omezeným pouze na data snímku specifických virtuálních počítačů v cílovém uzlu.

Obvykle je tomuto uzlu poskytnut přístup z cílového uzlu, který vlastní zálohy virtuálního počítače, pomocí příkazu `set access`:

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

Tento příkaz například poskytuje uzlu s názvem `myMountNode` oprávnění k obnově souborů z virtuálního počítače s názvem `myTestVM`:

```
set access backup -TYPE=VM myTestVM myMountNode
```

Pokud tuto volbu vyberete, postupujte takto:

a. Zadejte název cílového uzlu (uzel, na kterém jsou místěny zálohy virtuálního počítače) v poli **Cílový uzel**.
b. Zadejte název uzlu, kterému je poskytnut omezený přístup, v poli **Uzel ověření**.
c. Zadejte heslo pro uzel, kterému je poskytnut omezený přístup, v poli **Heslo**.
d. Klepnutím na tlačítko **OK** uložte tato nastavení a ukončete dialogové okno informací o funkci IBM Spectrum Protect.

Když použijete tuto metodu, můžete vidět úplný seznam zálohovaných virtuálních počítačů. Avšak můžete obnovit pouze virtuální počítače, ke kterým byl uzlu udělen přístup. Kromě toho nejsou data snímku chráněna před vypršením platnosti na serveru. Výsledkem je, že není v této metodě podporována okamžitá obnova.

Přímo
Vyberte tuto volbu, chcete-li ověřit přímo do cílového uzlu.

Pokud tuto volbu vyberete, postupujte takto:

a. Zadejte název cílového uzlu (uzel, na kterém jsou místěny zálohy virtuálního počítače) v poli **Uzel ověření**.
b. Zadejte heslo pro cílový uzel v poli **Heslo**.
c. Klepnutím na tlačítko **OK** uložte tato nastavení a ukončete dialogové okno informací o funkci IBM Spectrum Protect.

Použít generování přístupu k heslu
Když je vybrána tato volba a pole s heslem je prázdné, agent zotavení ověří existující heslo uložené v registru. Pokud není vybrána, musíte heslo zadat ručně.

Chcete-li použít tuto volbu, musíte nejprve ručně nastavit počáteční heslo pro uzel, na kterém se má volba použít. Musíte zadat počáteční heslo, když se poprvé připojíte k uzlu IBM Spectrum Protect, zadáním hesla do pole **Heslo** a označením zaškrtávacího políčka **Použít generování hesla pro přístup**.

Avšak když použijete uzel lokálního modulu pro přesouvání dat jako **uzel ověření**, může být heslo již uloženo v registru. Proto označte zaškrtávací políčko **Použít generování hesla pro přístup** a nezadávejte heslo.

Agent zotavení se dotazuje určeného serveru na seznam chráněných virtuálních počítačů a ukazuje seznam.

3. Nastavte následující volby připojení, zálohy a obnovy klepnutím na volbu **Nastavení**:

Mezipaměť pro zápis virtuálního svazku
Agent zotavení spuštěný na hostiteli zástupce pro zálohování Windows ukládá změny dat vytvořené během připojení a okamžité obnovy. Tyto změny jsou uloženy na virtuálním svazku v mezipaměti pro zápis. Standardně je mezipaměť pro zápis povolena a uvádí cestu `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\` a maximální velikost mezipaměti je 90 % dostupného prostoru pro vybranou složku. Chcete-li zabránit zaplnění svazku systému, změňte mezipaměť pro zápis na cestu ve svazku jiném než systémový svazek.

Složka pro dočasné soubory
Zadejte cestu, kde jsou uloženy změny dat. Mezipaměť pro zápis musí být umístěna na lokální jednotce a nemůže být nastavena na cestu ve sdílené složce. Pokud je mezipaměť pro zápis zakázána nebo plná, pokus o spuštění relace okamžité obnovy nebo připojení selže.

Velikost mezipaměti
Uveďte velikost mezipaměti pro zápis. Maximální povolená velikost mezipaměti je 90 % dostupného prostoru pro vybranou složku.

Omezení: Chcete-li zabránit přerušení během zpracování obnovy, vylučte cestu k mezipaměti pro zápis ze všech nastavení ochrany pomocí antivirového softwaru.

Přístup k datům
Uveďte typ dat, ke kterým se má přistoupit. Používáte-li offline zařízení (jako je páska nebo virtuální pásková knihovna), musíte uvést použitelný datový typ.

Typ úložiště
Zadejte jedno z následujících úložných zařízení, ze kterých se má připojit snímek:

Disk/Soubor
Snímek je připojen z disku nebo souboru. Toto zařízené je předvolba.

Páska
Snímek je připojen z fondu úložišť pásek. Když vyberete tuto volbu, nebude možné připojit více snímků nebo spustit operaci okamžité obnovy.

VTL
Snímek je připojen z offline virtuální páskové knihovny. Souběžné relace připojení na stejné virtuální páskové knihovně jsou podporovány.

Poznámka: Když je změněn typ úložiště, musíte restartovat službu, aby změny nabyly účinnosti.

Zakázat ochranu vypršení platnosti
Během operace připojení je snímek na serveru IBM Spectrum Protect uzamčen pro ochranu před vypršením platnosti během operace. K vypršení platnosti může dojít, protože se další snímek přidá do připojené posloupnosti snímku. Tato hodnota uvádí, zda zakázat ochranu vypršení platnosti během operace připojení.

- Chcete-li ochránit snímek před vypršením platnosti, pak tuto volbu nevybírejte. Snímek na serveru IBM Spectrum Protect je uzamčen a snímek je chráněn před vypršením platnosti během operace připojení.
- Chcete-li zakázat ochranu vypršení platnosti, vyberte tuto volbu. Tato volba se vybere standardně. Snímek na serveru IBM Spectrum Protect není uzamčen a snímek není chráněn před vypršením platnosti během operace připojení. Výsledkem je vypršení snímku během operace připojení. Toto vypršení platnosti může vynést neočekávané výsledky a může mít negativní vliv na bod připojení. Například bod připojení se může stát nepoužitelným nebo může obsahovat chyby. Avšak vypršení neovlivní aktuální aktivní kopii. Aktivní kopie nemůže vypršet během operace.

  Když je snímek na cílovém replikačním serveru, snímek nelze uzamknout, protože je v režimu jen pro čtení. Pokus o uzamčení serverem způsobí selhání operace připojení. Chcete-li se vyhnout pokusu o uzamčení a zabránit takovému selhání, zakažte ochranu vypršení výběrem této volby.

Velikost čtení vpředu (v 16-KB blocích)
Uveďte počet přebytečných datových bloků načtených z úložného zařízení po odeslání požadavku na čtení do jednotlivého bloku. Výchozí hodnoty jsou následující:

- Disk nebo soubor: 64
- Páska: 1024
- VTL: 64

Maximální hodnoty pro všechna zařízení je 1024.

Velikost mezipaměti čtení vpřed (v blocích)
Uveďte velikost mezipaměti, kde se uloží přebytečné datové bloky. Výchozí hodnoty jsou následující:

- Disk nebo soubor: 10000
- Páska: 75000
- VTL: 10000

Poněvadž má každý snímek svou vlastní mezipaměť, ujistěte se o naplánování počtu současně připojených nebo obnovených snímků. Kumulativní velikost mezipaměti nesmí překročit 75000 bloků.

Časový limit ovladače (sekundy)
Tato hodnota uvádí dobu pro zpracování datových požadavků z ovladače systému souborů. Pokud není zpracování dokončeno včas, je požadavek zrušen a ovladači systému souborů je vrácena chyba. Zvažte zvýšení této hodnoty, když dojde k vypršení časového limitu. Vypršení časového limitu se může například vyskytnout, když je síť pomalá, úložné zařízení přetížené, nebo když se zpracovává více relací připojení nebo okamžité obnovy. Výchozí hodnoty jsou následující:

- Disk nebo soubor: 60
- Páska: 180
- VTL: 60

Klepněte na tlačítko **OK**, abyste uložili změny a ukončili **Nastavení**.

4. Ověřte, že každý uzel serveru IBM Spectrum Protect (uvedený pomocí voleb `Asnodename` a `Fromnode`) umožňuje odstranění záloh.

   Agent zotavení vytvoří nepoužívané dočasné objekty během operací. Volba serveru `BACKDELete=Yes` umožňuje tyto objekty odebírat, aby se nehromadily v uzlu.

   a) Přihlaste se k serveru IBM Spectrum Protect a spusťte v režimu příkazového řádku relaci administrativního klienta:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

   b) Zadejte následující příkaz:

   ```
   Query Node <nodename> Format=Detailed
   ```

   Ujistěte se, že výstup příkazu pro každý uzel zahrnuje následující příkaz:

   ```
   Backup Delete Allowed?: Yes
   ```

   Pokud není tento příkaz zahrnut, aktualizujte každý uzel pomocí následujícího příkazu:

   ```
   UPDate Node <nodename> BACKDELete=Yes
   ```

   Opětovným spuštěním příkazu `Query Node` pro každý uzel ověřte, že každý uzel umožňuje odstranění záloh.

5. Když použijete agenta zotavení v síti iSCSI a agent zotavení nepoužívá modul pro přesouvání dat, přejděte do souboru `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` a uveďte značku `[IMOUNT]` a parametr **`Target IP`**:

   ```
   [IMOUNT config]
   Target IP=<Adresa IP síťové karty na systému,
   který vystaví cíle iSCSI.>
   ```

   Například:

   ```
   [General config]
   param1
   ```

```
param2
...
[IMount config]
Target IP=9.11.153.39
```

Po přidání nebo změně parametru cílové adresy IP restartujte grafické rozhraní agenta zotavení nebo rozhraní příkazového řádku agenta zotavení.

Povolení zabezpečené komunikace agenta zotavení se serverem IBM Spectrum Protect

Pokud je server IBM Spectrum Protect nakonfigurován tak, aby používal protokol SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security), můžete umožnit agentovi zotavení, aby komunikoval se serverem pomocí tohoto protokolu.

Než začnete

Než začnete s konfigurací zabezpečené komunikace se serverem, zvažte následující požadavky:

- Každý server s povoleným zabezpečením SSL musí mít jedinečný certifikát. Může se jednat o jeden z těchto typů certifikátů:
  - Certifikát serveru podepsaný držitelem.
  - Certifikát vydaný certifikační autoritou třetí strany. Certifikát certifikační autority může být od společnosti, jako je Symantec nebo Thawte, nebo se může jednat o interní certifikát, který je udržován ve vaší společnosti.
- Z výkonnostních důvodů používejte protokoly SSL nebo TLS pouze v relacích, kde se požaduje zabezpečení. Zvažte přidání více prostředků procesoru na serverový systém kvůli správě zvýšeného počtu požadavků.
- Aby se klient mohl připojit k serveru, který používá protokol TLS verze 1.2, podpisový algoritmus certifikátu musí být SHA-1 (Secure Hash Algorithm) nebo novější. Pokud používáte certifikát podepsaný držitelem na serveru, který používá protokol TSL V1.2, musíte použít certifikát `cert256.arm`. Administrátor serveru IBM Spectrum Protect možná bude muset změnit výchozí certifikát na serveru.
- Chcete-li zakázat protokoly zabezpečení, které jsou méně bezpečné než protokol TLS 1.2, přidejte volbu **`SSLDISABLELEGACYtls yes`** do souboru `C:\windows\system32\fb.opt` nebo `C:\Windows\SysWOW64\fb.opt`. Protokol TLS 1.2 nebo novější pomáhá bránit útokům pomocí škodlivých programů.

Povolení zabezpečené komunikace pomocí certifikátu serveru IBM Spectrum Protect podepsaného držitelem

Pokud server IBM Spectrum Protect používá certifikát podepsaný držitelem, musíte získat kopii tohoto certifikátu od administrátora serveru a nakonfigurovat agenta zotavení tak, aby komunikoval se serverem pomocí protokolu SSL nebo TLS.

Informace o této úloze

Každý server generuje vlastní certifikát. Servery verze 6.3 a novější generují soubory s názvem `cert256.arm`, pokud server používá protokol TLS 1.2 nebo vyšší, nebo `cert.arm`, pokud server používá starší verzi protokolu SSL nebo TLS. Starší verze serveru než 6.3 generují soubory s názvem `cert.arm` bez ohledu na protokol. Musíte zvolit certifikát, který bude na serveru nastaven jako výchozí.

Soubor certifikátů je uložen na pracovní stanici serveru v adresáři instance serveru. Například `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. Pokud soubor certifikátů neexistuje, bude vytvořen po restartu serveru s těmito volbami.

Postup

Chcete-li povolit komunikaci přes protokoly SSL nebo TLS z agenta zotavení na server pomocí certifikátu podepsaného držitelem:

1. Připojte binární cestu produktu GSKit a cestu ke knihovně k proměnné prostředí PATH na klientovi.

   Například:

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
    C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```

2. Pokud konfigurujete protokol SSL nebo TLS na klientovi poprvé, musíte vytvořit databázi lokálních klíčů klienta dsmcert.kdb.

   V adresáři `C:\Windows\SysWOW64` spusťte příkaz **gsk8capicmd_64**, jak uvádí následující příklad:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   Zadané heslo se použije k zašifrování databáze klíčů. Toto heslo bude automaticky uloženo v zašifrované podobě v souboru pro dočasné ukládání (dsmcert.sth). Soubor pro dočasné ukládání je používán klientem pro načtení hesla databáze klíčů.
3. Získejte certifikát serveru podepsaný držitelem.
4. Importujte certifikát do databáze dsmcert.kdb. Musíte do databáze dsmcert.kdb importovat certifikáty pro všechny klienty.

   V adresáři `C:\Windows\SysWOW64` spusťte příkaz **gsk8capicmd_64**, jak uvádí následující příklad:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server název_serveru self-signed
   key"
   -file cesta_k_certifikátu -format ascii -trust enable
   ```

   Do databáze dsmcert.kdb lze přidat více certifikátů serveru, aby se klient mohl připojit k různým serverům. Různé certifikáty musí mít odlišné popisky. Používejte smysluplné popisky.

   Důležité: Pokud byl certifikát ztracen v případě zotavení serveru z havárie, server automaticky vygeneruje nový certifikát. Každý klient pak musí importovat nový certifikát.
5. Když je certifikát serveru přidán do databáze dsmcert.kdb, přidejte volbu `ssl yes` do souboru `C:\Windows\SysWOW64\fb.opt` a aktualizujte hodnotu volby `tcpport`.

   Důležité:

   Server má obvykle nastavena připojení přes protokoly SSL a TLS na jiném portu než jiná připojení než přes tyto protokoly. Neuvádějte jako hodnotu `tcpport` číslo portu používané pro jiné protokoly než SSL a TLS. Je-li hodnota `tcpport` chybná, agent zotavení se nemůže připojit k serveru.

   Nemůžete se připojit k jinému portu než SSL nebo TLS s agentem zotavení, který má povolen protokol SSL nebo TLS, nebo se připojit k portu SSL nebo TLS s agentem zotavení, který nemá protokol SSL nebo TLS povolen.
6. Nastavte správné porty protokolu SSL nebo TLS v následujících konfiguračních souborech agenta zotavení:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Povolení zabezpečené komunikace pomocí certifikátu třetí strany
Pokud server IBM Spectrum Protect využívá certifikační autoritu třetí strany, musíte získat kořenový certifikát této certifikační autority.

Informace o této úloze

Pokud byl certifikát vydán certifikační autoritou, jako např. Symantec či Thawte, je klient připraven používat protokoly SSL nebo TLS a můžete následující kroky konfigurace vynechat. Chcete-li získat seznam předem nainstalovaných kořenových certifikátů CA, vyhledejte **kořenové certifikáty certifikační autority** v Centru znalostí IBM.

Pokud nebyl certifikát vydán předinstalovaným kořenovým certifikátem nebo se jedná o certifikát vnitřní certifikační autority udržovaný v rámci společnosti, musíte agenta zotavení nakonfigurovat tak, aby komunikoval se serverem pomocí protokolu SSL nebo TLS.

Postup

Chcete-li povolit komunikaci přes protokoly SSL nebo TLS z agenta zotavení na server pomocí certifikátu certifikační autority:

1. Připojte binární cestu produktu GSKit a cestu ke knihovně k proměnné prostředí PATH.

   Například:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. Pokud konfigurujete protokol SSL nebo TLS na klientovi poprvé, musíte vytvořit databázi lokálních klíčů klienta dsmcert.kdb.

   Pro klienty v adresáři `C:\Windows\SysWOW64` spusťte příkaz **gsk8capicmd_64**, jak uvádí následující příklad:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   Zadané heslo se použije k zašifrování databáze klíčů. Toto heslo bude automaticky uloženo v zašifrované podobě v souboru pro dočasné ukládání (dsmcert.sth). Soubor pro dočasné ukládání je používán klientem pro načtení hesla databáze klíčů.

3. Získejte certifikát certifikační autority.

4. Importujte certifikát do databáze dsmcert.kdb. Musíte do databáze dsmcert.kdb importovat certifikáty pro všechny klienty.

   Pro klienty v adresáři `C:\Windows\SysWOW64` spusťte příkaz **gsk8capicmd_64**, jak uvádí následující příklad:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
   -file cesta_ke_kořenovému_certifikátu_CA -format ascii -trust enable
   ```

   Do databáze dsmcert.kdb lze přidat více certifikátů serveru, aby se klient mohl připojit k různým serverům. Různé certifikáty musí mít odlišné popisky. Používejte smysluplné popisky.

   Důležité: Pokud byl certifikát ztracen v případě zotavení serveru z havárie, server automaticky vygeneruje nový certifikát. Každý klient musí importovat nový certifikát.

5. Když je certifikát serveru přidán do databáze dsmcert.kdb, přidejte volbu `ssl yes` do souboru `C:\Windows\SysWOW64\fb.opt` a aktualizujte hodnotu volby `tcpport`.

   Důležité:

   Server má obvykle nastavena připojení přes protokoly SSL a TLS na jiném portu než jiná připojení než přes tyto protokoly. Neuvádějte jako hodnotu `tcpport` číslo portu používané pro jiné protokoly než SSL a TLS. Je-li hodnota `tcpport` chybná, agent zotavení se nemůže připojit k serveru.

   Nemůžete se připojit k jinému portu než SSL nebo TLS s agentem zotavení, který má povolen protokol SSL nebo TLS, nebo se připojit k portu SSL nebo TLS s agentem zotavení, který nemá protokol SSL nebo TLS povolen.

6. Nastavte správné porty protokolu SSL nebo TLS v následujících konfiguračních souborech agenta zotavení:

   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Národní nastavení

Nastavení národního prostředí identifikuje jazyk použitý pro rozhraní, zprávy a nápovědu online.

Grafická rozhraní produktu Data Protection for VMware

Fráze "Grafické rozhraní produktu Data Protection for VMware" se vztahuje na následující grafická rozhraní:

- grafické rozhraní produktu Data Protection for VMware vSphere zpřístupněné ve webovém prohlížeči
- grafické rozhraní modulu IBM Spectrum Protect vSphere Client plug-in ve webovém klientovi vSphere

Grafická uživatelská rozhraní produktu Data Protection for VMware nepodporují běh v prostředí, které obsahuje nekonzistentní nastavení národního prostředí v rámci procesorů, na nichž běží grafické uživatelské rozhraní produktu Data Protection for VMware, klient VMware vSphere Client a server IBM Spectrum Protect.

Uveďte stejná nastavení národního prostředí v rámci systémů, na nichž běží grafické uživatelské rozhraní produktu Data Protection for VMware, klient VMware vSphere a server IBM Spectrum Protect.

Když poprvé přistoupíte ke stránce nápovědy grafického rozhraní produktu Data Protection for VMware pomocí odkazu "Další informace", nápověda se zobrazí v jazyce, který uvádí nastavení národního prostředí systému, který spouští grafické rozhraní produktu Data Protection for VMware. Nápověda se nezobrazí v jazyce uvedeném národním prostředím klienta VMware vSphere při prvním přístupu k této nápovědě. V této situaci, po zobrazení stránky nápovědy grafického rozhraní produktu Data Protection for VMware klepněte na alespoň dva odkazy v nápovědě a pak nápovědu zavřete. Příště, až spustíte nápovědu pomocí odkazu "Další informace", se zobrazí v jazyce, který uvádí nastavení národního prostředí klienta VMware vSphere.

Rozhraní pro obnovu souborů produktu IBM Spectrum Protect

Jazyk obsahu rozhraní a příkazového řádku zprávy je určen nastavením jazyka webového prohlížeče, který přistoupil k rozhraní obnovy souborů IBM Spectrum Protect.

Pro chybové zprávy, které jsou zaprotokolovány do souboru `fr_api.log`, rozhraní pro obnovu souborů IBM Spectrum Protect používá jazyk, který je uveden nastavením národního prostředí systému, který spouští grafické rozhraní produktu Data Protection for VMware vSphere.

Aktivita souboru protokolu

Produkt Data Protection for VMware během operací instalace, zálohy, připojení a obnovy vytváří a upravuje několik souborů protokolu.

Soubory protokolu produktu Data Protection for VMware jsou soubory s prostým textem používající příponu `.sf`.

Windows Protokoly jsou umístěny do tohoto adresáře:
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`
Adresáře obsahují podadresář pro každou komponentu Data Protection for VMware. Podadresářem agenta zotavení je například `\mount` a podadresářem rozhraní příkazového řádku agenta Recovery Agent je `\shell`.
Soubory protokolu můžete vyhledat z nabídky **Windows** > **Start** výběrem položek **Ovládací panel** > **Vyhledávání** a zadáním řetězce `*.log`.

Linux Protokoly jsou umístěny v obou z uvedených cest:
`<user.home>/tivoli/tsm/ve/mount/log`
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`
Soubory protokolu můžete vyhledat zadáním následujícího příkazu:

```
find /opt/tivoli/ -name "*.log"
```

Důležité: Existující soubory protokolu jsou přepisovány při každém spuštění instalace. Pokud zjistíte problém instalace a musíte produkt přeinstalovat, načtěte před zopakováním instalace existující soubor `TDPVMwareInstallation.log` z adresáře `%allusersprofile%`.

Poznámka: Když je služba Data Protection for VMware spuštěná, několik souborů protokolu je zadrženo v otevřeném stavu. V důsledku toho někteří správci souborů nezobrazují aktuální stav těchto souborů a mohou vykázat velikost souboru nula. Výběr nebo otevření jednoho z těchto souborů vynutí na správci souborů aktualizaci podrobností tohoto souboru.

Soubory protokolu agenta zotavení

Soubor protokolu agenta zotavení je TDP_FOR_VMWARE_MOUNT*nnn*.sf. Soubor protokolu s nejnovějšími daty je uložen v souboru protokolu s číslem *040* (TDP_PRO_VMWARE_MOUNT040.sf). Když velikost souboru dosáhne maximálního limitu, vytvoří se nový soubor protokolu. Název souboru protokolu bude stejný, ale jeho číslo se o jednotku sníží. Konkrétně, data v souboru protokolu s číslem *040* se zkopírují do souboru protokolu s číslem *039*. Soubor protokolu s číslem *040* obsahuje nejnovější data. Když soubor protokolu *040* opět dosáhne maximální velikosti, obsah souboru *039* se přesune do souboru *038* a informace ze souboru *040* opět přejdou do souboru *039*.

Soubory protokolu grafického rozhraní produktu Data Protection for VMware

Komponenta Data Protection for VMware vSphere umístí soubory protokolu do tohoto adresáře:

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Když shromažďujete soubory protokolu, ujistěte se, že zahrnujete všechny podadresáře v komprimovaném souboru.

Soubory protokolu rozhraní příkazového řádku produktu Data Protection for VMware

Komponenta rozhraní příkazového řádku produktu Data Protection for VMware umisťuje soubory protokolu do následujícího adresáře:

Windows `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/logs`

Když shromažďujete soubory protokolu, ujistěte se, že zahrnujete všechny podadresáře v komprimovaném souboru.

Soubory protokolu rozhraní pro obnovu souborů IBM Spectrum Protect

Rozhraní pro obnovu souborů IBM Spectrum Protect zachycuje chybové zprávy do souborů `fr_api.log`, `fr_gui.log` a `messages.log`. Tyto soubory jsou v následujícím výchozím adresáři:

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Můžete změnit název a umístění tohoto souboru `fr_api.log` nastavením voleb `API_LOG_FILE_NAME` a `API_LOG_FILE_LOCATION` v souboru aktivit protokolu obnovení souboru (`FRLog.config`).

Operace obnovení souboru jsou také vykázány serverem IBM Spectrum Protect. Tyto zprávy můžete vyhledat pomocí klienta administrativního příkazového řádku serveru.

- Chcete-li spustit administrativní relaci klienta v režimu příkazového řádku, zadejte tento příkaz na pracovní stanici:

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  Zadáním příkazu **DSMADMC** s volbami **-ID** a **-PASSWORD**, jak je uvedeno, nebudete vyzváni k zadání ID uživatele a hesla.

- Chcete-li prohledávat souhrnnou rozšířenou tabulku SQL a zobrazit výsledky operací obnovy souboru, zadejte příkaz **select** z klienta administrativního příkazového řádku:

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  Můžete zúžit hledání zahrnutím jednoho nebo více následujících kritérií do příkazu select:

  - * ENTITY='*DATA_MOVER_NODE_NAME*'
  - * AS_ENTITY='*DATA_CENTER_NODE_NAME*'
  - * SUB_ENTITY='*VM_HOST_NAME*'
  - * START_TIME='*rrrr-MM-dd HH:mm:ss*'

Například:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
and START_TIME>'2017-03-11 17:30:00'
```

Kritérium START_TIME podporuje dotazy s následujícími znaky: rovná se (=), menší než (<) nebo větší než (>).

- Chcete-li prohledávat tabulku protokolu aktivit a zobrazit události o operacích obnovy souborů, zadejte příkaz **select** z klienta administrativního příkazového řádku:

```
select * from ACTLOG
```

Můžete zúžit hledání zahrnutím jednoho nebo více následujících kritérií do příkazu select:

– * NODENAME='*DATA_CENTER_NODE_NAME*'

– * DATE_TIME='*yyyy-MM-dd HH:mm:ss*'

Například:

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
```

Uveďte hodnoty *DATA_MOVER_NODE_NAME* a *DATA_CENTER_NODE_NAME* velkými písmeny.

Kritérium DATE_TIME podporuje dotazy s následujícími znaky: rovná se (=), menší než (<) nebo větší než (>).

Spuštění a provoz služeb produktu Data Protection for VMware

Standardně se při spuštění operačního systému Windows spustí agent zotavení pod účtem lokálního systému.

Spuštění služeb agenta zotavení na systému Microsoft Windows
Když spustíte agenta zotavení z nabídky Start systému Windows, je služba automaticky zastavena. Když je agent zotavení spuštěný z nabídky Start dokončen, je služba automaticky spuštěna. Kromě toho neposkytuje služba pro tyto operační systémy grafické rozhraní. Chcete-li použít grafické uživatelské rozhraní, přejděte do nabídky Windows Start a vyberte volby **Všechny programy** > **IBM Spectrum Protect** > **Data Protection for VMware** > **zotavení**.

rozhraní příkazového řádku produktu Data Protection for VMware
Pomocí následující úlohy můžete ověřit, že je komponenta rozhraní příkazového řádku produktu Data Protection for VMware spuštěná:

Windows Přejděte do nabídky **Start** > **Control Panel** > **Administrativní nástroje** > **Služby** a ověřte, že je stav komponenty `rozhraní příkazového řádku produktu Data Protection for VMware` Spuštěno.

Linux Přejděte do adresáře skriptů (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) a zadejte tento příkaz:

```
./vmclid status
```

- Pokud není démon spuštěn, zadejte tento příkaz a spusťte ho ručně:

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

K zastavení a spuštění démona lze také použít tyto inicializační skripty:

```
./vmclid stop
./vmclid start
```

Dodatek A. Rozšířené konfigurační úlohy

Musíte ručně nakonfigurovat a ověřit každou komponentu pomocí dostupných aplikačních rozhraní.

Než začnete
Před pokračováním úlohy se ujistěte, že existují následující kritéria:

- Server IBM Spectrum Protect musí být k dispozici pro registraci uzlů.
- Grafické rozhraní produktu Data Protection for VMware vSphere je nainstalováno na systému, který splňuje nezbytné předpoklady na operační systém. Musí mít síťovou připojitelnost k následujícím systémům:
  - Záložní server vStorage
  - Server IBM Spectrum Protect
  - Server vCenter

Postup

1. Přihlaste se k serveru IBM Spectrum Protect a dokončete úlohy popsané v tématu t_ve_cfg_regtsmnodes.dita.
2. Přihlaste se k záložnímu serveru vStorage a dokončete úlohy popsané v tématu “Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere” na stránce 83.
3. Přihlaste se k systému, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere, a dokončete úlohy popsané v tématu “Konfigurace rozhraní příkazového řádku produktu Data Protection for VMware v prostředí vSphere” na stránce 91.
4. Na systému, na kterém je nainstalováno grafické rozhraní produktuData Protection for VMware vSphere, spusťte klienta vSphere přihlaste se k nástroji vCenter.

   Pokud je již klient vSphere spuštěn, musíte ho zastavit a restartovat.
5. Přejděte do domovského adresáře v klientovi vSphere. Klepněte na ikonu grafického rozhraní produktu Data Protection for VMware vSphere v panelu Řešení a aplikace.

   Tip: Pokud není ikona zobrazena, nebylo grafické rozhraní produktu Data Protection for VMware vSphere registrováno, nebo došlo k chybě připojení.

   a. V nabídce klienta vSphere přejděte na volbu **Moduly plug-in** > **Spravovat moduly plug-in** a spusťte správce modulu plug-in.

   b. Pokud můžete vyhledat grafické rozhraní produktu Data Protection for VMware vSphere a došlo k chybě připojení, ověřte konektivitu k počítači, kde je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere, zadáním příkazu `ping`.

Výsledky
Grafické rozhraní produktu Data Protection for VMware vSphere je připraveno na operace zálohování a obnovy.

Nastavení uzlů produktu IBM Spectrum Protect v prostředí vSphere

Tato procedura popisuje, jak ručně registrovat uzly na server IBM Spectrum Protect a udělit oprávnění zástupce pro tyto uzly v prostředí vSphere.

Než začnete

Důležité:

Informace o této úloze
Všechny kroky v této proceduře jsou dokončené na serveru IBM Spectrum Protect.

Tip: Tato úloha může být také dokončena pomocí průvodce konfigurací nebo zápisníku úpravy konfigurace grafického rozhraní produktu Data Protection for VMware vSphere. Spusťte grafické rozhraní produktu Data Protection for VMware vSphere otevřením webového prohlížeče a přechodem na grafické rozhraní webového serveru. Například:

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

Přihlaste se pomocí jména uživatele a hesla vCenter.

- Pro počáteční konfiguraci přejděte na volbu **Konfigurace** > **Spustit průvodce konfigurací**.
- Pro existující konfiguraci přejděte na volbu **Konfigurace** > **Upravit konfiguraci**.

Postup

1. Přihlaste se k serveru IBM Spectrum Protect a spusťte v režimu příkazového řádku relaci administrativního klienta:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. Zadejte příkaz `REGister Node` a registrujte následující uzly na server IBM Spectrum Protect:
   a) Uzel představující VMware vCenter (Uzel nástroje vCenter):

   ```
   REGister Node MY_VCNODE <heslo pro MY_VCNODE>
   ```

   b) Uzel komunikující mezi produktem IBM Spectrum Protect a grafickým rozhraním produktu Data Protection for VMware vSphere (Uzel VMCLI):

   ```
   REGister Node MY_VMCLINODE <heslo pro MY_VMCLINODE>
   ```

   c) Uzel představující datové středisko a místo uložení dat virtuálního počítače (uzel datového střediska):

   ```
   REGister Node MY_DCNODE <heslo pro MY_DCNODE>
   ```

   d) Uzel "přesunující data" z jednoho systému do jiného (uzel modulu pro přesouvání dat):

   ```
   REGister Node MY_DMNODE <heslo pro MY_DMNODE>
   ```

   Upozornění: Při registraci uzlů na server IBM Spectrum Protect nepoužívejte parametr `userid`.

3. Zadejte příkaz `GRant PROXynode` a definujte vztahy zástupců pro tyto uzly:

   Zapamatujte si: Cílové uzly vlastní data a uzly agenta jednají jménem cílových uzlů. Udělení oprávnění zástupce cílovému uzlu může uzel agenta provést operace zálohy a obnovy pro cílový uzel.

   a) Zadáním následujícího příkazu udělte uzlu Uzel nástroje vCenter oprávnění zástupce:

   ```
   GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
   ```

   Tento příkaz udělí uzlům `MY_DCNODE` a `MY_VMCLINODE` oprávnění pro zálohu a obnovu virtuálních počítačů jménem `MY_VCNODE`.

   b) Zadáním následujícího příkazu udělte uzlu uzel datového střediska oprávnění zástupce:

   ```
   GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
   ```

   Tento příkaz udělí uzlům `MY_VMCLINODE` a `MY_DMNODE` oprávnění pro zálohu a obnovu virtuálních počítačů jménem `MY_DCNODE`.

   c) (Volitelné) Udělte oprávnění zástupce jakýmkoli dalším uzlům uzel datového střediska nebo uzlům modulu pro přesouvání dat ve vašem prostředí.

   d) Zadáním příkazu `Query PROXynode` serveru IBM Spectrum Protect ověřte vztahy zástupce. Očekávaný výstup příkazu je následující:

Očekávaný výstup příkazu je:

```
Cílový uzel       Uzel agenta
--------------    ----------------------------
MY_VCNODE           MY_DCNODE  MY_VMCLINODE
MY_DCNODE           MY_VMCLINODE  MY_DMNODE
```

Jak pokračovat dále

Po úspěšném nastavení uzlů produktu IBM Spectrum Protect je další ruční konfigurační úlohou nastavení uzlů modulu pro přesouvání dat, jak je popsáno v tématu “Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere” na stránce 83.

Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere

Pokud odlehčujete pracovní zátěž zálohování na záložní server vStorage v prostředí vSphere, můžete použít průvodce modulem pro přesouvání dat k nastavení řady uzlů modulu pro přesouvání dat pro spuštění operace a přesunutí dat na server IBM Spectrum Protect.

Než začnete

Nastavení uzlů modulu pro přesouvání dat vyžaduje změny konfigurace, spuštění nezbytných služeb a ověření nastavení.

Tyto úlohy můžete provést pomocí grafického rozhraní modulu plug-in, které zjednodušuje a zrychluje vytvoření řady uzlů modulu pro přesouvání dat. Případně můžete práci provést ručně. Další informace viz část “Ruční nastavení uzlů modulu pro přesouvání dat v prostředí vSphere ” na stránce 84.

Ve standardním prostředí grafického rozhraní produktu Data Protection for VMware se použije samostatný soubor `dsm.opt` (Windows) nebo sekce souboru `dsm.sys` (Linux) pro každý uzel modulu pro přesouvání dat. Když se na záložním serveru vStorage pro zabránění duplikaci dat používá více uzlů modulů pro přesouvání dat a tyto uzly mají oprávnění k přesunu dat pro stejný uzel uzel datového střediska, tak každý soubor `dsm.opt` nebo sekce souboru `dsm.sys` musí zahrnovat odlišnou hodnotu pro volbu `dedupcachepath`.

Uzel modulu pro přesouvání fyzických dat k záloze a obnově dat obvykle používá SAN. Pokud uzel modulu pro přesouvání dat nakonfigurujete pro přímý přístup ke svazkům úložišť, vypněte automatické přiřazení písmene jednotky. Pokud přiřazení písmen nevypnete, může klient na uzlu modulu pro přesouvání dat porušit RDM (Raw Data Mapping) virtuálních disků. Pokud je RDM virtuálních disků poškozeno, záloha selže.

Omezení: Produkt Data Protection for VMware nepodporuje plánování záložního serveru vStorage (použitého jako modul pro přesouvání dat) pro zálohování sebe sama. Ujistěte se, že je záložní server vStorage vyloučen z vlastních plánů. K provedení zálohy virtuálního počítače obsahujícího záložní server vStorage použijte jiný záložní server vStorage.

Potřebujete-li provést některou z výše uvedených úprav, prohlédněte si téma "Ruční nastavení uzlů modulu pro přesouvání dat v prostředí vSphere."

Informace o této úloze

Použijte modul plug-in vSphere ke konfiguraci uzlů modulu pro přesouvání dat.

Postup

1. V modulu vSphere vyberte IBM Spectrum Protect .
2. Na kartě **Konfigurovat** vyberte volbu **Moduly pro přesouvání dat**.
3. Na panelu **Přidat modul pro přesouvání dat** vyberte datové středisko v rozevírací nabídce.
4. Podle potřeby upravte následující pole:

- **Název modulu pro přesouvání dat**: Název uzlu, který je již vyplněn navrhovaným názvem založeným na předponě uzlu, názvu uzlu datového střediska, názvu modulu pro přesouvání dat a rostoucím číslem.
- **Název hostitele modulu pro přesouvání dat**
- **Uživatel služby vCenter**: Již vyplněný jménem uživatele, který registroval modul plug-in.
- **Heslo služby vCenter**

Po dokončení nastavení klepněte na tlačítko **Přidat**.

5. Obrazovka **Výsledky** ukazuje:
   - Název nakonfigurovaného modulu pro přesouvání dat.
   - Umístění souboru voleb. Modul pro přesouvání dat můžete nakonfigurovat tak, že upravíte tento soubor.
   - Umístění souborů protokolu.
   - Použité výchozí volby.
6. Nyní můžete otestovat modul pro přesouvání dat pomocí karty **IBM Spectrum Protect > Konfigurovat moduly pro přesouvání dat** . Instalaci můžete také ověřit výběrem modulu pro přesouvání dat a klepnutím na tlačítko **Ověřit** nebo kontrolou stavu při příštím přidání modul pro přesouvání dat.
7. Modul pro přesouvání dat můžete přidat do plánu pomocí karty **IBM Spectrum Protect > Plány**.

Ruční nastavení uzlů modulu pro přesouvání dat v prostředí vSphere

Pokud odlehčujete pracovní zátěž zálohování na záložní server vStorage v prostředí vSphere, můžete ručně nastavit uzly modulu pro přesouvání dat pro spuštění operace a přesunutí dat na server IBM Spectrum Protect.

Uzel modulu pro přesouvání fyzických dat k záloze a obnově dat obvykle používá SAN. Jestliže konfigurujete uzly modulu pro přesouvání dat pro přímý přístup ke svazům úložišť, vypněte automatické přiřazení písmen jednotky. Pokud přiřazení písmen nevypnete, může klient na uzlu modulu pro přesouvání dat porušit RDM (Raw Data Mapping) virtuálních disků. Pokud je RDM virtuálních disků poškozeno, záloha selže.

Požadované služby: Modul pro přesouvání dat požaduje službu Client Acceptor, službu agenta vzdáleného klienta a službu plánovače modulu pro přesouvání dat, jak je popsáno v následujících krocích. Pokud modul pro přesouvání dat odeberete z datového střediska, odinstalujte a odstraňte tyto služby pro modul pro přesouvání dat.

Důležité: Pokud je modul pro přesouvání dat nainstalován na stejném systému Windows jako grafické rozhraní produktu Grafické rozhraní produktu Data Protection for VMware vSphere a během konfigurace modulu pro přesouvání dat byla vybrána volba **Vytvořit služby**, následující kroky se nepožadují.

Ve standardním prostředí grafického rozhraní produktu Data Protection for VMware se použije samostatný soubor `dsm.opt` (Windows) nebo sekce souboru `dsm.sys` (Linux) pro každý uzel modulu pro přesouvání dat. Když se na záložním serveru vStorage pro zabránění duplikaci dat používá více uzlů modulů pro přesouvání dat a tyto uzly mají oprávnění k přesunu dat pro stejný uzel uzel datového střediska, tak každý soubor `dsm.opt` nebo sekce souboru `dsm.sys` musí zahrnovat odlišnou hodnotu pro volbu `dedupcachepath`. Nejlepších výsledků dosáhnete uvedením různých voleb `schedlogname` a `errorlogname` pro každý soubor `dsm.opt` nebo sekci souboru `dsm.sys`.

Poznámka: Všechny kroky v této proceduře jsou dokončeny na záložním serveru vStorage.

Uzel modulu pro přesouvání fyzických dat k záloze a obnově dat obvykle používá SAN. Pokud uzel modulu pro přesouvání dat nakonfigurujete pro přímý přístup ke svazkům úložišť, vypněte automatické přiřazení písmene jednotky. Pokud přiřazení písmen nevypnete, může klient na uzlu modulu pro přesouvání dat porušit RDM (Raw Data Mapping) virtuálních disků. Pokud je RDM virtuálních disků poškozeno, záloha selže.

Omezení: Produkt Data Protection for VMware nepodporuje plánování záložního serveru vStorage, který se používá jako modul pro přesouvání dat, pro zálohování sebe sama. Ujistěte se, že je záložní server

vStorage vyloučen z vlastních časových plánů. Použijte odlišný záložní server vStorage, abyste zálohovali záložní server vStorage, který se používá jako modul pro přesouvání dat.

Ke shromáždění informací budete muset

Informace o modulu pro přesouvání musí být shromážděny z průvodce konfigurací hostitele grafického uživatelského rozhraní v době vytváření uzlu modulu pro přesouvání dat v průvodci. Prohlédněte si téma “Pracovní list konfigurace” na stránce 27, kde naleznete požadované informace. Dříve než ručně nakonfigurujete modul pro přesouvání dat, shromážděte a poznamenejte si následující informace:

- jméno uživatele a heslo pro vCenter
- název uzlu modulu pro přesouvání dat
- heslo modulu pro přesouvání dat
- ukázky voleb modulu pro přesouvání dat

Název modulu pro přesouvání dat a ukázky voleb můžete shromáždit v následné fázi pomocí následujícího procesu:

1. Otevřete webový prohlížeč a zadejte adresu webového serveru grafického uživatelského rozhraní: například `https://guihost.mycompany.com:9081/TsmVMwareUI/`
2. Přihlaste se pomocí jména uživatele a hesla pro vCenter a ujistěte se, že je vybrán režim konfigurace.
3. V průvodci konfigurací přejděte na stránku **Uzly modulu pro přesouvání dat**.
4. Vyhledejte požadovaný modul pro přesouvání dat a klepněte na volbu **Zobrazit**.
5. Zkopírujte ukázky voleb z karty **Zobrazit** do souboru voleb.
6. Pokud to vaše prostředí vyžaduje, upravte tyto volby podle potřeby.

Minimální sady požadovaných voleb jsou pro každou platformu poskytovány v těchto tématech:

- “Nastavení uzlů modulu pro přesouvání dat Windows” na stránce 85
- “Nastavení uzlů modulu pro přesouvání dat Linux” na stránce 87

Nastavení uzlů modulu pro přesouvání dat Windows

Můžete použít záložní server vStorage k nastavení uzlů modulu pro přesouvání dat Windows.

Než začnete

Shromážděte informace popsané v konceptuálním tématu “Ruční nastavení uzlů modulu pro přesouvání dat v prostředí vSphere ” na stránce 84.

Postup

1. Zkopírujte volby z ukázkového souboru voleb `dsm.opt` pro modul pro přesouvání dat do souboru voleb, který je umístěný v adresáři `C:\Program Files\Tivoli\TSM\baclient`. Pojmenujte soubor voleb po modulu pro přesouvání dat: například `dsm.PREFIX_DATACENTER_DM.opt`.
2. Je-li to pro vaše prostředí vyžadováno, můžete tyto volby podle potřeby aktualizovat. Popis voleb naleznete v tématu Odkaz na volby klienta.

   V případě operací okamžitého přístupu, okamžité obnovy nebo připojení (obnova souborů) přidejte `VMISCSISERVERADDRESS` do souboru voleb modulu pro přesouvání dat. Uveďte adresu IP serveru iSCSI síťové karty na záložním serveru vStorage používanou pro přenos dat iSCSI během okamžitých operací. Fyzická karta síťového rozhraní (NIC), která je svázána se zařízením iSCSI na hostiteli ESX, musí být na stejné podsíti jako NIC záložního serveru vStorage použitá pro přenos iSCSI.
3. Zadejte následující příkaz, chcete-li nastavit uživatele a heslo VMware vCenter pro uzel modulu pro přesouvání dat: `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`

   Informace o požadovaných právech administrátora naleznete v technické poznámce 7047438

4. Tato procedura používá průvodce konfigurací grafického uživatelského rozhraní klienta produktu IBM Spectrum Protect k nastavení služby Client Acceptor a služby plánovače. Standardně se služba agenta vzdáleného klienta rovněž nastaví pomocí průvodce. Pokud pro tuto úlohu používáte obslužný program konfigurace služby klienta produktu IBM Spectrum Protect (`dsmcutil`), musíte také nainstalovat službu agenta vzdáleného klienta. Nastavte službu Client Acceptor a službu plánovače modulu pro přesouvání dat pomocí následujících úloh:
5. Nastavte službu Client Acceptor a službu plánovače modulu pro přesouvání dat pomocí následujících úloh:
   - Tato procedura používá průvodce Konfigurace grafického rozhraní klienta IBM Spectrum Protect k nastavení služby Client Acceptor a služby plánovače. Standardně se služba agenta vzdáleného klienta rovněž nastaví pomocí průvodce. Pokud pro tuto úlohu používáte obslužný program konfigurace služby klienta IBM Spectrum Protect (**`dsmcutil`**), ujistěte se, že máte také instalovanou službu agenta vzdáleného klienta.

     Spusťte průvodce konfigurací klienta nástroje IBM Spectrum Protect z nabídky souboru přechodem do **Nástroje** > **Průvodce nastavením**:

     – Vyberte volbu **Nápověda ke konfiguraci webového klienta TSM**. Zadejte požadované informace.

       a. Ve volbě `Kdy chcete, aby se služba spustila?` vyberte **Automaticky při zavádění systému Windows**.

       b. Ve volbě `Přejete si spustit službu po dokončení tohoto průvodce?` vyberte **Ano**.

     Když je operace úspěšně dokončena, vraťte se na úvodní stránku průvodce.

     Tip: Pokud na stejném počítači konfigurujete více než jeden uzel modulu pro přesouvání dat, musíte pro každou instanci příjemce klienta uvést jinou hodnotu portu.

     – Vyberte volbu `Nápověda ke konfiguraci plánovače klienta TSM`. Zadejte požadované informace.

       a. Při zadávání názvu plánovače se ujistěte, že vyberte volbu **Použít démona služby Client Acceptor ke správě plánovače**.

       b. Ve volbě `Kdy chcete, aby se služba spustila?` vyberte **Automaticky při zavádění systému Windows**.

       c. Ve volbě `Přejete si spustit službu po dokončení tohoto průvodce?` vyberte **Ano**.

Výsledky

Chcete-li ověřit nastavení konfigurace:

1. Spusťte relaci příkazového řádku modulu pro přesouvání dat s parametry příkazového řádku `-asnodename` a `-optfile`: `dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt`

   Ujistěte se, že nejste po počátečním přihlášení vyzváni k zadání hesla.

   Upozornění: Chcete-li zabránit selhání plánovače IBM Spectrum Protect, ujistěte se, že volba `asnodename` není nastavena v souboru `dsm.opt` (Windows) nebo v sekci souboru `dsm.sys` (Linux). Plánovač se dotáže serveru IBM Spectrum Protect na časové plány přidružené k `nodename` (uzel modulu pro přesouvání dat), nikoliv `asnodename` (uzel produktu uzel datového střediska). Je-li volba `asnodename` nastavena v souboru `dsm.opt` nebo v sekci souboru `dsm.sys`, dotáží se časové plány přidružené k `asnodename` (nikoliv k `nodename`). Jako výsledek operace plánování selžou.

Postupujte takto:

1. Ověřte připojení k serveru IBM Spectrum Protect zadáním následujícího příkazu:

```
dsmc query session
```

Tento příkaz zobrazuje informace o vaší relaci, včetně aktuálního názvu uzlu, je-li relace zavedena, informace o serveru a informace o připojení serveru.

2. Zadáním následujícího příkazu ověřte, že můžete zálohovat virtuální počítač:

```
dsmc backup vm vm1
```

kde vm1 je název virtuálního počítače.

3. Zadáním následujícího příkazu ověřte, že je záloha úspěšně dokončena:

```
dsmc query vm "*"
```

4. Zadáním následujícího příkazu ověřte, že lze virtuální počítač obnovit:

```
dsmc restore vm vm1 -vmname=vm1-restore
```

5. Ověřte, že jsou služba Client Acceptor a agent správně nastaveni:
   a. Ve webovém prohlížeči zadejte adresu modulu klienta IBM Spectrum Protect vSphere. Například:

```
https://guihost.mycompany.com/vsphere-client/
```

   b. Přihlaste se pomocí jména uživatele a hesla služby vCenter.
   c. Ve webovém klientovi vSphere klepněte na volby **IBM Spectrum Protect > Konfigurovat > Moduly pro přesouvání dat**.
   d. Ujistěte se, že ve sloupci **Stav** modulu pro přesouvání dat je uvedena hodnota **Ověřeno**. Je-li zde uvedena hodnota **Selhání**, podržte nad stavem ukazatel myši a zobrazte zprávu o selhání.

      Tip: Když se změní adresa IP na systému, na kterém je instalováno grafické rozhraní produktu Data Protection for VMware vSphere, musíte postupovat takto:

   e. Dokončete úlohy popsané v části Odstraňování problémů
   f. Nastavte službu Client Acceptor znovu, aby se grafické uživatelské rozhraní produktu Data Protection for VMware vSphere stalo dostupným pro operace. Jinak zobrazuje správce modulu plug-in stav grafického rozhraní produktu Data Protection for VMware vSphere jako zakázaný.

Související úlohy

“Rozšířené konfigurační úlohy” na stránce 81
Musíte ručně nakonfigurovat a ověřit každou komponentu pomocí dostupných aplikačních rozhraní.

Nastavení uzlů modulu pro přesouvání dat Linux

Můžete použít záložní server vStorage k nastavení uzlů modulu pro přesouvání dat Linux.

Než začnete

Shromážděte informace popsané v konceptuálním tématu “Ruční nastavení uzlů modulu pro přesouvání dat v prostředí vSphere ” na stránce 84.

Informace o této úloze

Postup

1. Použijte verzi jazyka Java nainstalovanou od IBM, která je umístěná na systému Linux v umístění instalace Java: `export JAVA_HOME=/opt/tivoli/tsm/tdpvmware/common/jre/jre`
2. Nastavte příslušné proměnné prostředí.
   a. Ujistěte se, že je proměnná prostředí JAVA_HOME správně exportována:

```
JAVA_HOME=<jre-or-jdk-install-dir>
```

b. Ujistěte se, že je proměnná prostředí PATH správně exportována:

```
export PATH=$PATH:$JAVA_HOME/jre/bin
```

3. Nastavte službu Client Acceptor a službu plánovače modulu pro přesouvání dat pomocí následujících úloh:

- **Nakonfigurujte modul pro přesouvání dat na systému Linux.**

  V případě modulu pro přesouvání dat na systému Linux použijte odpovídající přístup ke konfiguraci pro váš operačního systém a verzi Linux: **systemd**, nebo **SysV**. Ty jsou popsány v následujících sekcích.

  Chcete-li nakonfigurovat modul pro přesouvání dat na systému Linux pomocí `systemd`, postupujte takto:

  V tomto ukázkovém postupu je jako název uzlu použito `PREFIX_DATACENTER_DM`.

  a. Zkopírujte následující skript do adresáře `/etc/systemd/system` a pojmenujte jej `dsmcad@PREFIX_DATACENTER_DM.service`

```
#!/bin/bash
#
# (C) Copyright IBM Corporation 2018
#
# chkconfig: 35 95 5
# popis: démon IBM Spectrum Protect Client Acceptor
#
### BEGIN INIT INFO
# Provides: dsmcad
# Required-Start: $local_fs $remote_fs $network $syslog
# Required-Stop:
# Default-Start: 3 5
# Default-Stop: 0 1 2 6
# Short-Description: IBM Spectrum Protect Client Acceptor Daemon
# Description: Start dsmcad to enable scheduler and Web GUI.
### END INIT INFO
# SERVERNAME referenced in dsm.$SERVERNAME.opt and dsm.sys
SERVERNAME=LNX11L_DATACENTER_DM1
DSMCAD_DIR=/opt/tivoli/tsm/client/ba/bin
DSMCAD_BIN=$DSMCAD_DIR/dsmcad
OPTION_FILE=$DSMCAD_DIR/dsm.$SERVERNAME.opt
PID_FILE=/var/run/dsmcad-$SERVERNAME.pid
export JAVA_HOME=/opt/tivoli/tsm/tdpvmware/common/jre/jre
export LD_LIBRARY_PATH=$DSMCAD_DIR:$JAVA_HOME/lib/amd64/classic
export PATH=$JAVA_HOME/bin:$PATH
createPidFile()
{
  pid=`pgrep -f $OPTION_FILE`
  pidarr=($pid)
    if [ -n "${pidarr[1]}" ]
    then
       echo ${pidarr[1]} > $PID_FILE
    else
      echo ${pidarr[0]} > $PID_FILE
    fi
}
removePidFile()
{
  if [ -f $PID_FILE ]
  then
    rm -f $PID_FILE
  fi}
```

  Aktualizujte skript, aby byla hodnota SERVERNAME nastavena na název uzlu.

  b. Nemusíte provádět žádné změny ve skriptu. Chcete-li se ujistit, že skript má 664 oprávnění, zadejte příkaz `chmod 664 dsmcad@.service`

  c. Vytvořte textový soubor s názvem `dsm.PREFIX_DATACENTER_DM.opt` v adresáři `/opt/tivoli/tsm/client/ba/bin` a přidejte následující nastavení: `servername PREFIX_DATACENTER_DM`.

  d. Vytvořte soubor `dsm.sys` v adresáři `/opt/tivoli/tsm/client/ba/bin` a přidejte ukázky voleb modulu pro přesouvání dat.

Popis těchto voleb naleznete v tématu Popis voleb.

V případě operací okamžitého přístupu, okamžité obnovy nebo připojení (obnova souborů) musíte přidat VMISCSISERVERADDRESS do souboru voleb modulu pro přesouvání dat. Uveďte adresu IP serveru iSCSI síťové karty na záložním serveru vStorage používanou pro přenos dat iSCSI během okamžitých operací. Fyzická karta síťového rozhraní (NIC), která je svázána se zařízením iSCSI na hostiteli ESX, musí být na stejné podsíti jako NIC záložního serveru vStorage použitá pro přenos iSCSI.

e. Po vytvoření konfiguračních souborů uložte pověření vCenter, aby mohl modul pro přesouvání dat / server proxy pro připojení přistoupit k inventáři vCenter. Přejděte do adresáře `/opt/tivoli/tsm/client/ba/bin` a zadejte příkaz: `./dsmc set password –type=VM fullyqualifieddomainnameofvcenter vcenteruserid vcenterpassword`

Informace o požadovaných právech administrátora naleznete v technické poznámce 7047438

f. Chcete-li začít používat službu, zadejte následující tři příkazy:

- `systemctl daemon-reload`
- `systemctl enable dsmcad@PREFIX_DATACENTER_DM.service`
- `systemctl start dsmcad@PREFIX_DATACENTER_DM.service`

g. Když máte nakonfigurovaný jeden modul pro přesouvání dat, můžete použít grafické uživatelské rozhraní modulu plug-in webového klienta, abyste přidali další moduly pro přesouvání dat nebo servery proxy pro připojení.

Poznámka: Chcete-li zajistit, aby byla služba, která je přidružená k `PREFIX_DATACENTER_DM`, automaticky restartována při opětovném zavedení systému, spusťte příkaz `systemctl enable dsmcad@PREFIX_DATACENTER_DM.service`

Chcete-li zastavit službu, proveďte příkaz: `systemctl stop dsmcad@PREFIX_DATACENTER_DM.service`

Poznámka: Pokud odinstalujete komponentu IBM Spectrum Protect, musíte zastavit a odebrat přidružené služby:

- Pomocí výše uvedeného příkazu `stop` zastavte službu `dsmcad`.
- Zakažte službu pomocí příkazu: `systemctl disable dsmcad@PREFIX_DATACENTER_DM.service`
- Odeberte `dsmcad@.service` z adresáře `/etc/systemd/system`.

Chcete-li nakonfigurovat modul pro přesouvání dat na systému Linux pomocí SysV, postupujte takto:

V tomto ukázkovém postupu je jako název uzlu použito `PREFIX_DATACENTER_DM`.

a. Zkopírujte poskytnutý skript `rc.dsmcad` a aktualizujte skript, aby byla hodnota `SERVERNAME` nastavena na název uzlu: `SERVERNAME=PREFIX_DATACENTER_DM`

b. Uložte soubor jako `/etc/init.d/dsmcad.PREFIX_DATACENTER_DM`

c. Ujistěte se, že soubor má 775 oprávnění pomocí příkazu `chmod 755 dsmcad.PREFIX_DATACENTER_DM`

d. Vytvořte textový soubor s názvem `dsm.PREFIX_DATACENTER_DM.opt` v adresáři `/opt/tivoli/tsm/client/ba/bin` a přidejte následující nastavení: `servername PREFIX_DATACENTER_DM`.

e. Vytvořte soubor `dsm.sys` v adresáři `/opt/tivoli/tsm/client/ba/bin` a přidejte ukázky voleb modulu pro přesouvání dat.

Popis těchto voleb naleznete v tématu Popis voleb.

V případě operací okamžitého přístupu, okamžité obnovy nebo připojení (obnova souborů) musíte přidat VMISCSISERVERADDRESS do souboru voleb modulu pro přesouvání dat. Uveďte adresu IP serveru iSCSI síťové karty na záložním serveru vStorage používanou pro přenos dat iSCSI během okamžitých operací. Fyzická karta síťového rozhraní (NIC), která je svázána se

zařízením iSCSI na hostiteli ESX, musí být na stejné podsíti jako NIC záložního serveru vStorage použitá pro přenos iSCSI.

f. Po vytvoření konfiguračních souborů uložte pověření vCenter, aby mohl modul pro přesouvání dat / server proxy pro připojení přistoupit k inventáři vCenter. Přejděte do adresáře `/opt/tivoli/tsm/client/ba/bin` a zadejte příkaz: `./dsmc set password -type=VM fullyqualifieddomainnameofvcenter vcenteruserid vcenterpassword`

   Informace o požadovaných právech administrátora naleznete v technické poznámce 7047438

g. Přejděte do adresáře `/opt/tivoli/tsm/client/ba/bin` a proveďte příkaz: `./dsmc set password -type=VM fullyqualifieddomainname vcenteruserid vcenterpassword`

h. V závislosti na operačním systému proveďte následující příkazy:

   - Red Hat: `chkconfig - - add dsmcad.PREFIX_DATACENTER_DM`
   - SUSE: `chkconfig - - add dsmcad.PREFIX_DATACENTER_DM`
   - Ubuntu: `update-rc.d dsmcad.PREFIX_DATACENTER_DM defaults`

i. Spusťte příkaz: `service dsmcad.PREFIX_DATACENTER_DM start`

j. Když máte nakonfigurovaný jeden modul pro přesouvání dat, můžete použít grafické uživatelské rozhraní modulu plug-in webového klienta, abyste přidali další moduly pro přesouvání dat nebo servery proxy pro připojení.

Poznámka: Když spustíte příkaz `chkconfig`, služba `dsmcad.PREFIX_DATACENTER_DM` se restartujte při opětovném zavedení systému.

Chcete-li spustit službu: `service dsmcad.PREFIX_DATACENTER_DM start`

Chcete-li zastavit službu: `service dsmcad.PREFIX_DATACENTER_DM stop`

Poznámka: Pokud odinstalujete komponentu IBM Spectrum Protect, musíte zastavit přidružené služby:

- Pomocí výše uvedeného příkazu `stop` zastavte službu `dsmcad`.
- Zakažte službu pomocí příkazu: `systemctl disable dsmcad@PREFIX_DATACENTER_DM.service`, aby se odebraly pomocné soubory jako např. `/var/run/dsmcad.PREFIX_DATACENTER_DM.pid`.
- Na systému RHEL nebo SLES použijte příkaz: `chkconfig --del dsmcad.PREFIX_DATACENTER_DM`
- Na systému Ubuntu použijte příkaz: `update-rc.d dsmcad.PREFIX_DATACENTER_DM remove`
- Odeberte soubory `dsmcad.*` z adresáře `/etc/init.d`.

Výsledky

1. Spusťte relaci příkazového řádku modulu pro přesouvání dat s parametry příkazového řádku `-asnodename` a `-optfile`: `dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt`

   Ujistěte se, že nejste po počátečním přihlášení vyzváni k zadání hesla.

   Upozornění: Chcete-li zabránit selhání plánovače IBM Spectrum Protect, ujistěte se, že volba `asnodename` není nastavena v souboru `dsm.opt` (Windows) nebo v sekci souboru `dsm.sys` (Linux). Plánovač se dotáže serveru IBM Spectrum Protect na časové plány přidružené k `nodename` (uzel modulu pro přesouvání dat), nikoliv `asnodename` (uzel produktu uzel datového střediska). Je-li volba `asnodename` nastavena v souboru `dsm.opt` nebo v sekci souboru `dsm.sys`, dotáží se časové plány přidružené k `asnodename` (nikoliv k `nodename`). Jako výsledek operace plánování selžou.

Postupujte takto:

1. Ověřte připojení k serveru IBM Spectrum Protect zadáním následujícího příkazu:

```
dsmc query session
```

Tento příkaz zobrazuje informace o vaší relaci, včetně aktuálního názvu uzlu, je-li relace zavedena, informace o serveru a informace o připojení serveru.

2. Zadáním následujícího příkazu ověřte, že můžete zálohovat virtuální počítač:

```
dsmc backup vm vm1
```

kde vm1 je název virtuálního počítače.

3. Zadáním následujícího příkazu ověřte, že je záloha úspěšně dokončena:

```
dsmc query vm "*"
```

4. Zadáním následujícího příkazu ověřte, že lze virtuální počítač obnovit:

```
dsmc restore vm vm1 -vmname=vm1-restore
```

5. Ověřte, že jsou služba Client Acceptor a agent správně nastaveni:
   a. Ve webovém prohlížeči zadejte adresu modulu klienta IBM Spectrum Protect vSphere. Například:

```
https://guihost.mycompany.com/vsphere-client/
```

   b. Přihlaste se pomocí jména uživatele a hesla služby vCenter.
   c. Ve webovém klientovi vSphere klepněte na volby **IBM Spectrum Protect > Konfigurovat > Moduly pro přesouvání dat**.
   d. Ujistěte se, že ve sloupci **Stav** modulu pro přesouvání dat je uvedena hodnota **Ověřeno**. Je-li zde uvedena hodnota **Selhání**, podržte nad stavem ukazatel myši a zobrazte zprávu o selhání.

      Tip: Když se změní adresa IP na systému, na kterém je instalováno grafické rozhraní produktu Data Protection for VMware vSphere, musíte postupovat takto:

   e. Dokončete úlohy popsané v části Odstraňování problémů
   f. Nastavte službu Client Acceptor znovu, aby se grafické uživatelské rozhraní produktu Data Protection for VMware vSphere stalo dostupným pro operace. Jinak zobrazuje správce modulu plug-in stav grafického rozhraní produktu Data Protection for VMware vSphere jako zakázaný.

Konfigurace rozhraní příkazového řádku produktu Data Protection for VMware v prostředí vSphere

Aktualizujte profil rozhraní příkazového řádku produktu Data Protection for VMware na systému, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere.

Než začnete

Profil (`vmcliprofile`) je umístěn v adresáři na systému, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 bitů: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

Informace o této úloze

Všechny kroky v této proceduře jsou dokončené na systému, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere.

Tip: Tato úloha může být také dokončena pomocí průvodce konfigurací nebo zápisníku konfigurace grafického rozhraní produktu Data Protection for VMware vSphere. Přejděte do okna Data Protection for VMware vSphere **Konfigurace** a klepněte na volbu **Spustit průvodce konfigurací** nebo **Upravit konfiguraci**.

Postup

1. Pomocí následujících nastavení aktualizujte profil:

   VE_TSMCLI_NODE_NAME
   Uveďte uzel, který připojuje komponentu rozhraní příkazového řádku produktu Data Protection for VMware k serveru IBM Spectrum Protect a uzlu agenta (`MY_VMCLINODE`).

   Omezení: Uzel Uzel VMCLI při komunikaci se serverem IBM Spectrum Protect nepodporuje protokol SSL nebo ověření LDAP.

   VE_VCENTER_NODE_NAME
   Uveďte virtuální uzel představující nástroj vCenter (`MY_VCNODE`).

   VE_DATACENTER_NAME
   Uveďte virtuální uzel mapující na datové středisko. Níže je uvedena správná syntaxe:
   `název_datového_střediska::název_uzlu_datového_střediska`

   - Hodnota `název_datového_střediska` rozlišuje velikost písmen.
   - Ujistěte se, že nastavíte tento parametr pro každé datové středisko ve vašem prostředí (`MY_DCNODE`).
   - Grafické rozhraní produktu Data Protection for VMware vSphere nepodporuje datová střediska se stejným názvem v nástroji vCenter.

   VE_TSM_SERVER_NAME
   Uveďte název hostitele nebo adresu IP serveru IBM Spectrum Protect.

   VE_TSM_SERVER_PORT
   Uveďte název portu, který se má použít pro server IBM Spectrum Protect. Výchozí hodnota je `1500`.

   Níže je uveden příklad profilu s těmito nastaveními:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. Nastavte heslo uzlu Uzel VMCLI v souboru `pwd.txt`.

   Jedná se o heslo pro uzel, který připojuje komponentu rozhraní příkazového řádku produktu Data Protection for VMware k serveru IBM Spectrum Protect a uzel modulu pro přesouvání dat. Je uveden pomocí parametru profilu VE_TSMCLI_NODE_NAME.

   a) Zadejte příkaz `echo` a vytvořte textový soubor obsahující heslo:
   Linux `echo password1 > pwd.txt`
   Windows `echo password1> pwd.txt`

   Windows Mezi heslem (`password1`) a znaménkem větší než (>) nesmí být mezera.

   b) Zadáním tohoto příkazu vmcli nastavte heslo pro uzel Uzel VMCLI.
   `vmcli -f set_password -I pwd.txt`

   Důležité:

   - Linux Příkaz `vmcli -f set_password` musíte zadat jako uživatel tdpvmware a ne jako uživatel root.
   - Windows Linux Pokud hodláte generovat sestavy na ochranu aplikace, musíte uvést parametr **`-type VMGuest`**, který označí, že heslo platí pro virtuální počítač. Například:

     ```
     vmcli -f set_password -type VMGuest -I password.txt
     ```

3. Ověřte, že je komponenta rozhraní příkazového řádku produktu Data Protection for VMware spuštěná:

Windows Klepněte na volby **Start** > **Ovládací panel** > **Administrativní nástroje** > **Služby** a ověřte, že je stav komponenty `rozhraní příkazového řádku produktu Data Protection for VMware` Spuštěno.

Linux Přejděte do adresáře skriptů (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) a zadejte tento příkaz:

```
./vmclid status
```

- Pokud je démon spuštěn, pokračujte krokem 4.
- Pokud není démon spuštěn, zadejte tento příkaz a spusťte ho ručně:

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  K zastavení a spuštění démona lze také použít tyto inicializační skripty:

  ```
  ./vmclid stop
  ./vmclid start
  ```

4. Zadejte tento příkaz vmcli a ověřte, že komponenta rozhraní příkazového řádku produktu Data Protection for VMware rozeznává konfiguraci uzlu produktu IBM Spectrum Protect:

   ```
   vmcli -f inquire_config -t TSM
   ```

5. Ověřte uzly a potvrďte, že nedošlo k žádným chybám konfigurace:
   a) Klepnutím na ikonu v okně Řešení a aplikace klienta nástroje vSphere spusťte grafické rozhraní produktu Data Protection for VMware vSphere.
   b) Přejděte do okna **Konfigurace**.
   c) Vyberte uzel v tabulce a klepněte na volbu **Ověřit vybraný uzel**. Informace o stavu jsou zobrazeny v podokně **Podrobnosti o stavu**.

Jak pokračovat dále

Windows Linux Po úspěšném dokončení tří ručních konfiguračních úloh popsaných v této části:

1. “Nastavení uzlů produktu IBM Spectrum Protect v prostředí vSphere” na stránce 81
2. “Nastavení uzlů modulu pro přesouvání dat pomocí grafického rozhraní modulu plug-in vSphere” na stránce 83

Nepožadují se žádné další konfigurační úlohy pro zálohování dat virtuálního počítače.

Kontrolní seznam konfigurace rozhraní příkazového řádku prostředí vSphere

Pomocí této procedury nakonfigurujte produkt Data Protection for VMware v prostředí vSphere pouze pomocí rozhraní příkazového řádku.

Postup

Dokončete Krok 1 a Krok 2 na serveru IBM Spectrum Protect.

1. Registrujte následující uzly na server IBM Spectrum Protect:
   a) Uzel představující VMware vCenter (Uzel nástroje vCenter):

   ```
   REGister Node MY_VCNODE <heslo pro MY_VCNODE>
   ```

   b) Uzel komunikující mezi produktem IBM Spectrum Protect a grafickým rozhraním produktu Data Protection for VMware vSphere (Uzel VMCLI):

   ```
   REGister Node MY_VMCLINODE <heslo pro MY_VMCLINODE>
   ```

   c) Uzel představující datové středisko a místo uložení dat virtuálního počítače (uzel datového střediska):

```
REGister Node MY_DCNODE <heslo pro MY_DCNODE>
```

d) Uzel "přesunující data" z jednoho systému do jiného (uzel modulu pro přesouvání dat):

```
REGister Node MY_DMNODE <heslo pro MY_DMNODE>
```

2. Definujte vztahy zástupce pro tyto uzly:

a) Zadáním následujícího příkazu udělte uzlu Uzel nástroje vCenter oprávnění zástupce:

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Tento příkaz udělí uzlům MY_DCNODE a MY_VMCLINODE oprávnění pro zálohu a obnovu virtuálních počítačů jménem MY_VCNODE.

b) Zadáním následujícího příkazu udělte uzlu uzel datového střediska oprávnění zástupce:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Tento příkaz udělí uzlům MY_VMCLINODE a MY_DMNODE oprávnění pro zálohu a obnovu virtuálních počítačů jménem MY_DCNODE.

c) (Volitelné) Udělte oprávnění zástupce jakýmkoli dalším uzlům uzel datového střediska nebo uzlům modulu pro přesouvání dat ve vašem prostředí.

d) Zadáním příkazu `Query  PROXynode` serveru IBM Spectrum Protect ověřte vztahy zástupce. Očekávaný výstup příkazu je následující:

```
Cílový uzel       Uzel agenta
--------------    ------------------------------
MY_VCNODE               MY_DCNODE  MY_VMCLINODE
MY_DCNODE             MY_VMCLINODE  MY_DMNODE
```

Dokončete kroky 3 až 9 na záložním serveru vStorage.

3. Nastavte odpovídající hodnoty pro následující volby modulu pro přesouvání dat:

- Windows V souboru voleb `dsm.opt` uveďte tyto volby.
- Linux V souboru voleb `dsm.sys` uveďte tyto informace, v sekci pro nástroj uzel modulu pro přesouvání dat.

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

Poznámka: Volba HTTPPORT je požadována pouze, když se používá více než jedna služba CAD (Client Acceptor Service). Pokud například existují dva uzly modulu pro přesouvání (a dvě služby Client Acceptor), pak musí soubor voleb pro každý uzel modulu pro přesouvání dat uvádět odlišnou hodnotu HTTPPORT.

Níže je uveden příklad souboru dsm.dm.opt s těmito volbami:

```
NODename MY_DMNODE
PASSWORDAccess   generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort                     1500
COMMMethod tcpip
HTTPPORT    1583
```

4. Zadáním následujícího příkazu ověřte připojení k serveru IBM Spectrum Protect:
   `dsmc query session`
5. Zadejte tento příkaz, chcete-li nastavit uživatele a heslo VMware vCenter pro uzel modulu pro přesouvání dat:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
6. Nastavte následující služby produktu IBM Spectrum Protect:
   - Windows
     a. Instalujte službu plánovače:
     ```
     dsmcutil install scheduler /name:"TSM Central Scheduler Service"
     /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
     ```
     b. Instalujte službu CAD:
     ```
     dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
     /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
     /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
     ```
     c. Instalujte službu agenta vzdáleného klienta:
     ```
     dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
     /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
     /partnername:"TSM CAD - MY_DMNODE" /startnow:no
     ```
   - Linux V souboru voleb `dsm.sys` uveďte v sekci pro nástroj uzel modulu pro přesouvání dat tuto volbu `managedservices`:
     Ujistěte se, že uvedete parametry `schedule` a `webclient`:
     ```
     managedservices schedule webclient
     ```
     Toto nastavení řídí příjemce klienta pro správu webového klienta i plánovače.
7. Linux
   Spusťte službu Client Acceptor Service:
   Instalační program vytvoří spouštěcí skript pro démona Client Acceptor (`dsmcad`) v `/etc/init.d`. Než může démon Client Acceptor spravovat úlohy plánovače nebo webového klienta, musí být spuštěn. Jako kořen použijte následující příkaz ke spuštění démona:
   ```
   service dsmcad start
   ```
   Chcete-li démonu Client Acceptor povolit, aby se automaticky spustil po restartu systému, přidejte službu takto, v příkazovém řádku shellu:
   ```
   # chkconfig --add dsmcad
   ```
8. Ověřte, že jsou služby produktu IBM Spectrum Protect správně nastaveny:
   a) Přihlaste se ke vzdálenému systému.
   b) Pomocí webového prohlížeče se připojte k systému HOST1 pomocí této adresy a portu:
   `http://HOST1.xyz.yourcompany.com:1581`

Dokončete Krok 10 na systému, na kterém je nainstalováno grafické rozhraní produktu Data Protection for VMware vSphere.

9. Nastavte odpovídající hodnoty pro následující volby v profilu komponenty rozhraní příkazového řádku produktu Data Protection for VMware (`vmcliprofile`):
   ```
   VE_TSMCLI_NODE_NAME
   VE_VCENTER_NODE_NAME
   VE_DATACENTER_NAME
   VE_TSM_SERVER_NAME
   VE_TSM_SERVER_PORT
   ```

Níže je uveden příklad profilu s těmito volbami:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

Profil se nachází v následujících adresářích:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 bitů: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

a) Nastavte heslo pro uzel Uzel VMCLI:

1) Zadejte příkaz `echo` a vytvořte textový soubor obsahující heslo:

Linux
```
echo password1 > pwd.txt
```

Windows
```
echo password1> pwd.txt
```

2) Zadáním tohoto příkazu vmcli nastavte heslo pro uzel Uzel VMCLI.

Důležité: Linux Tento příkaz musíte zadat jako uživatel tdpvmware a ne jako uživatel root.

```
vmcli -f set_password -I pwd.txt
```

b) Ověřte, že je komponenta rozhraní příkazového řádku produktu Data Protection for VMware spuštěná:
Windows Z příkazového řádku Windows zadejte tento příkaz:
`net start`
Linux Zadejte tento příkaz:
`./vmclid status`

c) Zadejte tento příkaz vmcli a ověřte, že komponenta rozhraní příkazového řádku produktu Data Protection for VMware rozeznává konfiguraci uzlu produktu IBM Spectrum Protect:

```
vmcli -f inquire_config -t TSM
```

Pokyny pro konfiguraci pásky

Přezkoumejte tyto pokyny, než se pokusíte provést operace zálohování v úložišti pásek.

Příprava na zálohování na pásku

Windows Linux Než se pokusíte provést zálohu na pásku, musí být pro páskové zálohy na serveru IBM Spectrum Protect nastaveny následující parametry:

1. Definujte třídu správy:

```
define mgmtclass <název domény> <název sady zásad> <název třídy mgmtclass>
```

Například:

```
define mgmtclass tape tape DISK
```

2. Definujte skupinu kopií:

```
define copygroup <název domény> <název sady zásad> <název třídy mgmtclass>
destination=<název oblasti stgpool>
```

Například:

```
define copygroup tape tape DISK destination=Diskpool
```

3. Activujte sadu zásad:

```
activate policyset <název domény> <název sady zásad>
```

Například:

```
activate policyset tape tape
```

Během konfigurace fyzické pásky existují dodatečné konfigurační požadavky. Metadata IBM Spectrum Protect (řídicí soubory) musíte vždy ponechat na disku a skutečná zálohovaná data virtuálního počítače na pásce.

- Použijte volbu VMMC k uložení zálohování VMware (a řídicím souborům VMware) s třídou správy jinou, než je výchozí třída správy.
- Použijte volbu VMCTLMC k určení třídy správy, za účelem použití výhradně řídicí soubory pro VMware během zálohování VMware. Třída správy, kterou určíte, přepíše výchozí třídu správy. Také přepíše třídu správy určenou pomocí volby VMMC. Třída správy VMCTLMC musí určovat fond diskových úložišť, bez migrace na pásku.
- Volba VMMC se vždy používá k řízení uchování na zálohách virtuálních počítačů. Tato volba se vztahuje jak na konfigurace disků, tak i na konfigurace pásek. Volba VMCTLMC se nepoužívá pro uchování řídicích souborů. Řídicí a datové soubory jsou součástí stejného seskupení, a společně jim vypršela platnost na základě zásady uchování volby VMMC. Když jsou obě volby nastaveny, použije se volba VMMC pro datové soubory a volba VMCTLMC se použije pro řídicí soubory.

Omezení: Operace obnovy, které používají agenty úložišť v konfiguracích bez sítě LAN, mohou obnovit soubory z fondu úložišť kopie, ačkoli je možné data získat z primárního fondu úložišť. Toto se může stát, pokud je požadavek na obnovu pro specifický soubor, nebo pokud požadavek na obnovu nepoužívá metodu bez dotazu a primární kopie souboru je uložena ve fondu úložišť, který není přístupný přes cestu bez sítě LAN. Toto může také ovlivnit situace bez obnovy, jako jsou např. operace zálohování Data Protection for VMware. V prostředí Data Protection for VMware je disk upřednostňovaná metoda úložiště pro řídicí soubory virtuálního počítače, jako např. připojení není potřeba k obnově souboru během procesů přírůstkového zálohování. Tyto řídicí soubory virtuálního počítače nepotřebují pouze umístění na disku, ale neměly by se zálohovat do fondu úložišť kopie, který je k dispozici přes cestu bez sítě LAN. Pokud potřebují, připojení pásky se použije k obnově souborů během přírůstkového zálohování bez sítě LAN z klienta Data Protection for VMware.

Používá-li prostředí serveru IBM Spectrum Protect migraci disku na pásku, zvažte před migrováním následující pokyny:

- Nastavte fond diskových úložišť MIGDELAY na hodnotu, která podporuje nejvíce požadavků na připojení, jež se uspokojí z disku. Vzorky obvyklého použití označují, že vysoké procento obnovení jednotlivých souborů se vyskytují během několika dnů. Například během 3 až 5 dnů od doby, kdy byl soubor naposledy upraven. Proto zvažte uchování dat na disku po tuto krátkou dobu, abyste optimalizovali operace obnovení.

  Kromě toho, pokud spolu s fondem diskových úložišť používáte zabránění duplikaci, nastavte volbu MIGDELAY, která vyhovuje častým úplným zálohováním virtuálních počítačů. Nemigrujte data z fondu úložišť se zabráněnou duplikací na pásku do té doby, než jsou provedena alespoň dvě úplná zálohování pro virtuální počítač. Když se data přesunou na pásku, není již nadále bráněno v duplikaci. Pokud jsou například úplná zálohování spouštěna týdně, zvažte nastavení hodnoty volby MIGDELAY na alespoň 10 dní. Toto nastavení zajistí, že každá úplná záloha identifikuje a použije duplicitní data z předchozích záloh předtím, než se přesune na pásku.
- Použijte fond úložišť souborů třídy zařízení spíše než fond úložišť třídy zařízení DISK. Obvyklá hodnota pro velikost svazku uvedená parametrem MAXCAPACITY třídy zařízení je 8 gigabajtů až 16 gigabajtů. Pro přidružený fond úložišť zvažte použití kolokace podle souborového prostoru. Každý virtuální počítač, který je zálohován, je znázorněn jako oddělený souborový prostor na serveru IBM Spectrum Protect. Kolokace podle souborového prostoru chrání data před hromadným přírůstkovým zálohováním pro daný

virtuální počítač ve stejném svazku (soubor na disku). Když se vyskytne migrace na pásku, kolokace podle souborového prostoru vyhledá hromadná přírůstková zálohování pro daný virtuální počítač na fyzické pásce.

K nastavení hodnoty režimu pásky použijte dialogové okno **Nastavení**.

Operace zálohy se stane přerušenou, když požaduje operace připojení nebo okamžité obnovy stejné páskové úložiště, které současně používá operace zálohy.

Linux Ruční konfigurace zařízení iSCSI v systému Linux

Tato procedura popisuje, jak nakonfigurovat systém Linux, který se používá během operace připojení zařízení iSCSI. Snímek virtuálního počítače je připojen z úložiště serveru IBM Spectrum Protect.

Než začnete

Během připojení iSCSI se vytvoří cíl iSCSI na systému agenta zotavení. Iniciátor Microsoft iSCSI se na systému agenta zotavení nepožaduje.

Tip: Otevřený iniciátor iSCSI se poskytuje se serverem Red Hat Enterprise Linux a SUSE Linux Enterprise Server.

Přezkoumejte následující požadavky iSCSI, než budete pokračovat v této úloze:

- Můžete se připojit k cíli iSCSI z libovolného systému, abyste vytvořili svazek, který bude obsahovat zálohovaná data. Tento svazek můžete připojit z jiného systému.
- Iniciátor iSCSI je vyžadován na jakémkoli systému, který se musí připojit k cíli iSCSI.
- Na systému, kde se mají obnovit data, musí být nainstalován iniciátor iSCSI.
- Pokud má svazek rozpětí několika disků, musíte připojit všechny požadované disky. Při použití zrcadlených svazků připojte pouze jeden zrcadlený disk. Připojení jednoho disku zabrání operaci synchronizace, která zabírá čas.

Informace o této úloze

Tímto postupem nakonfigurujete systém Linux, který se použije během operace připojení zařízení iSCSI:

Postup

1. Zaznamenejte název iniciátoru iSCSI na systému, kde se mají data obnovit.

   Název iniciátoru iSCSI je umístěn v souboru `/etc/iscsi/initiatorname.iscsi`. Je-li hodnota `InitiatorName=` prázdná, vytvořte název iniciátoru s pomocí následujícího příkazu:

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   Zde je ukázkový název iniciátoru:

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. Přidejte název iniciátoru do souboru `/etc/iscsi/initiatorname.iscsi`.

   a) Upravte soubor `/etc/iscsi/initiatorname.iscsi` pomocí příkazu **`vi`**. Například:

   ```
   twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
   ```

   b) Aktualizujte parametr **`InitiatorName=`** názvem iniciátoru. Například:

   ```
   InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

3. Postupujte takto na systému, kde je instalován agent zotavení (nebo cíl iSCSI):

   a) Spusťte grafické rozhraní agenta zotavení. Dokončete dialogová okna `Vybrat server IBM Spectrum Protect` a `Vybrat snímek` a klepněte na tlačítko **Připojit**.

   b) V dialogovém okně `Zvolit cíl připojení` vyberte volbu `Připojit na cíl iSCSI`.

c) Vytvořte název cíle. Ujistěte se, že je jedinečný, a že ho můžete identifikovat ze systému, na kterém je spuštěn iniciátor iSCSI. Například:

```
iscsi-mount-tsm4ve
```

d) Zadejte název iniciátoru iSCSI, který byl zaznamenán v kroku 1, a klepněte na tlačítko **OK**.

e) Ověřte, že je svazek, který jste právě připojili, zobrazen v poli `Připojené svazky`.

4. Vyhledejte a spusťte program iniciátora iSCSI na systému iniciátora, který byl vybrán v kroku 1:

a) Ověřte, zda je služba iSCSI spuštěná zadáním tohoto příkazu:
Red Hat Enterprise Linux:

```
service iscsi status
```

SUSE Linux Enterprise Server:

```
service open-iscsi status
```

Pokud služba není spuštěná, zadáním tohoto příkazu službu spusťte:

Red Hat Enterprise Linux:

```
service iscsi start
```

SUSE Linux Enterprise Server:

```
service open-iscsi start
```

b) Připojte se k cíli iSCSI zadáním tohoto příkazu:

```
iscsiadm -m discovery -t sendtargets -p <adresa IP/název hostitele
systému zotavení> --login
```

c) Ověřte, zda je nové prosté zařízení k dispozici zadáním tohoto příkazu:

```
fdisk -l
```

5. Připojte systém souborů:

Pro svazek, který není svazkem LVM, zadejte následující příkazy. V tomto příkladu je novým zařízením `/dev/sdb1`:

```
mkdir /mountdir
mount /dev/sdb1 /mountdir
```

Pro svazek LVM postupujte na hostu systému Linux takto:

a. Ujistěte se, že je skript `vgimportclone` k dispozici na systému Linux. Tento skript není dodáván se základním (výchozím) balíkem LVM. Výsledkem může být to, že nemusíte aktualizovat balík LVM na úroveň, která poskytuje tento skript.

b. Zadejte příkaz **vgimportclone** a zahrňte nový základní název skupiny svazků (`VolGroupSnap01`). Například:

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```

c. Zadejte příkaz **lvchange**, abyste logický svazek označili jako aktivní. Například:

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```

d. Zadejte příkaz k připojení svazku:

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. Po dokončení operace obnovy souborů zadejte tyto příkazy:

- Pro svazky jiné než LVM zadejte následující příkazy:
  a. Zrušte připojení systému souborů:

     ```
     umount /dev/sdb1 /mountdir
     ```

  b. Odeberte svazek. Pokud je svazek částí skupiny svazků, nejprve odeberte svazek z dané skupiny svazků pomocí následujícího příkazu:

     ```
     vgreduce <vaše_skupina_svazků> /dev/sdb1
     ```

     Pak zadejte tento příkaz, abyste odebrali svazek:

     ```
     pvremove /dev/sdb1
     ```

  c. Odhlaste se z jednotlivého cíle:

     ```
     iscsiadm --mode node --targetname <target_name> --logout
     ```

  d. Odhlaste se ze všech cílů:

     ```
     iscsiadm --mode node --logout
     ```

- Pro svazek LVM postupujte na hostu systému Linux takto:
  a. Zrušte připojení systému souborů:

     ```
     unmount /mountdir
     ```

  b. Odeberte logický svazek:

     ```
     lvm lvremove LogVol00
     ```

  c. Odeberte skupiny svazků:

     ```
     lvm vgremove VolGroupSnap01
     ```

  d. Odhlaste se z jednotlivého cíle:

     ```
     iscsiadm --mode node --targetname <target_name> --logout
     ```

  e. Odhlaste se ze všech cílů:

     ```
     iscsiadm --mode node --logout
     ```

Windows Ruční konfigurace zařízení iSCSI v systému Windows

Tato procedura popisuje, jak nakonfigurovat systém Windows, který se používá během operace připojení zařízení iSCSI. Snímek je připojen z úložiště serveru IBM Spectrum Protect.

Než začnete

Přezkoumejte následující požadavky iSCSI, než budete pokračovat v této úloze:

- Během připojení iSCSI se vytvoří cíl iSCSI na systému agenta zotavení. Můžete se připojit k cíli iSCSI z libovolného systému, abyste vytvořili svazek, který bude obsahovat zálohovaná data. Tento svazek můžete také připojit z jiného systému.
- Iniciátor iSCSI je vyžadován na jakémkoli systému, který se musí připojit k cíli iSCSI.
- Ujistěte se, že je na systému, kde se mají obnovit data, nainstalován iniciátor iSCSI.
- Iniciátor Microsoft iSCSI se na systému agenta zotavení nepožaduje.

Přezkoumejte následující požadavky na disk a svazek, než budete pokračovat v této úloze:

- Pokud má svazek rozpětí několika disků, musíte připojit všechny požadované disky. Při použití zrcadlených svazků připojte pouze jeden zrcadlený disk. Připojení jednoho disku zabrání operaci synchronizace, která zabírá čas.
- Při použití více dynamických disků na záložním systému jsou tyto disky přiřazeny ke stejné skupině. Jako výsledek může při nasazení pouze jednoho disku správce disků Windows uvážit některé disky jako chybějící a vydat chybovou zprávu. Tuto zprávu ignorujte. Data na záložním disku jsou stále přístupná, dokud se na jiném disku nachází některá data. Tento problém je možné vyřešit připojením všech dynamických disků.

Informace o této úloze
Tímto postupem nakonfigurujete systém Windows, který se použije během operace připojení zařízení iSCSI:

Postup

1. V systému agenta zotavení otevřete port 3260 v bráně firewall sítě LAN a klienta systému Windows.
   Zaznamenejte název iniciátoru iSCSI na systému, kde se mají data obnovit.

   Název iniciátoru iSCSI se zobrazí v okně konfigurace iniciátoru iSCSI ovládacího panelu. Například:

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. Postupujte takto na systému, kde je instalován agent zotavení (nebo cíl iSCSI):
   a) Spusťte grafické rozhraní agenta zotavení. Dokončete dialogová okna **Vybrat server IBM Spectrum Protect** a **Vybrat snímek** a klepněte na tlačítko **Připojit**.
   b) V dialogovém okně **Zvolit cíl připojení** vyberte volbu **Připojit na cíl iSCSI**.
   c) Vytvořte název cíle. Ujistěte se, že je jedinečný, a že ho můžete identifikovat ze systému, na kterém je spuštěn iniciátor iSCSI. Například:

   ```
   iscsi-mount-tsm4ve
   ```

   d) Zadejte název iniciátoru iSCSI, který byl zaznamenán v kroku 1, a klepněte na tlačítko **OK**.
   e) Ověřte, že je svazek, který jste právě připojili, zobrazen v poli **Připojené svazky**.
   f) Když použijete agenta zotavení v síti iSCSI a agent zotavení nepoužívá modul pro přesouvání dat, přejděte do souboru `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` a uveďte značku `[IMOUNT]` a parametr **`Target IP`**:

   ```
   [IMOUNT config]
   Target IP=<Adresa IP síťové karty na systému,
   který vystaví cíle iSCSI.>
   ```

   Například:

   ```
   [General config]
   param1
   param2
   ...
   [IMount config]
   Target IP=9.11.153.39
   ```

   Po přidání nebo změně parametru cílové adresy IP restartujte grafické rozhraní agenta zotavení nebo rozhraní příkazového řádku agenta zotavení.
3. Vyhledejte a spusťte program iniciátora iSCSI na systému iniciátora, který byl vybrán v kroku 1:
   a) Připojte se k cíli iSCSI:
      1) Na kartě cíle zadejte adresu TCP/IP agenta zotavení (iSCSI target) použitou v kroku 2 v dialogovém okně **Cíl:**. Klepněte na tlačítko **Rychlé připojení**.

2) Dialogové okno **Rychlé připojení** zobrazí cíl, který odpovídá názvu cíle určenému v kroku 2c. Pokud není již připojen, vyberte tento cíl a klepněte na tlačítko **Připojit**.

b) Na systém iniciátora přejděte na **Ovládací panel** > **Administrativní nástroje** > **Správa počítačů** > **Úložiště** > **Správa disků**.

1) Pokud je připojený cíl iSCSI vypsán jako **Type=Foreign**, klepněte pravým tlačítkem myši na volbu **Cizí disk** a vyberte volbu **Importovat cizí disky**. Je zvolena volba **Cizí skupina disků**. Klepněte na tlačítko **OK**.

2) Další obrazovka ukazuje typ, stav a velikost cizího disku. Klepněte na tlačítko **OK** a počkejte na import disku.

3) Po dokončení importu disku stiskněte tlačítko **F5** (obnovit). Snímek připojeného iSCSI je viditelný a obsahuje přiřazené písmeno jednotky. Pokud nejsou písmena jednotek přiřazována automaticky, klepněte pravým tlačítkem myši na požadovanou oblast a vyberte volbu **Změnit písmena jednotek nebo cesty**. Klepněte na tlačítko **Přidat** a vyberte písmeno jednotky.

4. Otevřete program Windows Explorer (nebo jiný obslužný program) a procházejte připojený snímek pro operaci obnovy souborů.
5. Po obnově souboru postupujte takto:
   a) Odpojte každý cíl iSCSI pomocí dialogového okna **Vlastnosti iniciátoru iSCSI**.
   b) Odpojte svazek z kroku 2 výběrem svazku v grafickém rozhraní agenta zotavení a klepněte na tlačítko **Odpojit**.

Linux Ruční konfigurace uzly serveru proxy pro připojení na systému Linux

Postupujte takto, abyste přidali uzel serveru proxy pro připojení do vzdáleného systému Linux.

Než začnete

Ve standardním prostředí grafického rozhraní produktu Data Protection for VMware vSphere se použije samostatná sekce souboru `dsm.sys` pro každý uzel serveru proxy pro připojení. Všechny kroky v této proceduře dokončíte pomocí modulu pro přesouvání dat, který je nainstalován na záložním serveru.

Informace o této úloze

Tato úloha nastavuje uzly serveru proxy pro připojení aktualizováním voleb modulu pro přesouvání dat a ověřením připojitelnosti k serveru IBM Spectrum Protect.

Postup

1. V souboru voleb `dsm.sys` uveďte tyto informace, v sekci pro nástroj uzel serveru proxy pro připojení.

   NODENAME
   Uveďte název pro dříve definovaný uzel serveru proxy pro připojení. Plány produktu IBM Spectrum Protect jsou přidružené k tomuto uzlu.

   PASSWORDACCESS
   Uveďte volbu GENERATE, takže je heslo generováno automaticky (místo vyzvání uživatele).

   MANAGEDSERVICES
   Tuto volbu uveďte, chcete-li řídit příjemce klienta pro správu webového klienta i plánovače (`webový klient plánu`).

   TCPSERVERADDRESS
   Uveďte adresu TCP/IP serveru IBM Spectrum Protect.

   TCPPORT
   Uveďte adresu portu TCP/IP serveru IBM Spectrum Protect.

   COMMMETHOD
   Uveďte komunikační metodu, kterou má použít server IBM Spectrum Protect. Pro uzly serveru proxy pro připojení musíte uvést TCP/IP jako komunikační metodu. Pokud uvedete jinou metodu, operace selžou.

HTTPPORT
Tato volba uvádí adresu portu TCP/IP TCP/IP a musíte ji uvést pouze tehdy, když použijete více než jednu službu Client Acceptor. Pokud například existují dva uzly serveru proxy pro připojení (a dvě služby Client Acceptor), pak musí soubor voleb pro každý uzel serveru proxy pro připojení dat uvádět odlišnou hodnotu HTTPPORT.

Omezení: Nepovolujte volbu Bez sítě LAN (ENABLELANFREE YES) v souboru `dsm.sys`. Tato volba není podporována pro uzly serveru proxy připojení.

Níže je uveden příklad souboru dsm.sys s těmito nastaveními:

```
Servername     tsm_server1
        NODename datacenter1_MP_LNX
        PASSWORDAccess   generate
        MANAGEDServices schedule webclient
        TCPServeraddress tsmserver.myco.com
        TCPPort                    1500
        COMMMethod tcpip
        HTTPPORT    1583
```

2. Zadejte tento příkaz, abyste nastavili uživatele a heslo VMware pro uzel serveru proxy pro připojení:
`dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
3. Spusťte relaci příkazového řádku modulu pro přesouvání dat s parametry příkazového řádku `-asnodename` a `-optfile`:
`dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
Ujistěte se, že nejste po počátečním přihlášení vyzváni k zadání hesla.

Upozornění: Chcete-li zabránit selhání plánovače IBM Spectrum Protect, ujistěte se, že volba `asnodename` není nastavena v sekci souboru `dsm.sys` (Linux). Plánovač se dotáže serveru IBM Spectrum Protect na časové plány přidružené k `nodename` (uzel serveru proxy pro připojení), nikoliv `asnodename` (uzel datového střediska). Je-li volba `asnodename` nastavena v souboru `dsm.sys`, dotáží se časové plány přidružené k `asnodename` (nikoliv k `nodename`). Jako výsledek operace plánování selžou.

4. Zadáním následujícího příkazu ověřte připojení k serveru IBM Spectrum Protect:
`dsmc query session`
Tento příkaz zobrazuje informace o vaší relaci, včetně aktuálního názvu uzlu, je-li relace zavedena, informace o serveru a informace o připojení serveru.
5. Nastavte službu CAD (Client Acceptor Service) a službu plánovače modulu pro přesouvání dat dokončením těchto úloh:
   - V souboru voleb `dsm.sys` uveďte tyto informace, v sekci pro nástroj uzel serveru proxy pro připojení:
     – Uveďte volbu `managedservices` s těmito dvěma parametry:
     ```
     managedservices schedule webclient
     ```
     Toto nastavení řídí příjemce klienta pro správu webového klienta i plánovače.
     – Chcete-li směrovat informace o plánu a chybě souborů protokolu jiných, než jsou výchozí soubory, uveďte volby `schedlogname` a `errorlogname`. Každá volba musí obsahovat úplnou cestu a název souboru, do kterého se uloží informace protokolu. Například:
     ```
     schedlogname /vmsched/dsmsched_mp_lnx.log
     errorlogname /vmsched/dsmerror_mp_lnx.log
     ```
   - Spusťte službu Client Acceptor Service:
     Instalační program vytvoří spouštěcí skript pro démona Client Acceptor (`dsmcad`) v `/etc/init.d`. Než může démon Client Acceptor spravovat úlohy plánovače nebo webového klienta, musí být spuštěn. Jako kořen použijte následující příkaz ke spuštění démona:
     ```
     service dsmcad start
     ```

Chcete-li démonu Client Acceptor povolit, aby se automaticky spustil po restartu systému, přidejte službu takto, v příkazovém řádku shellu:

```
# chkconfig --add dsmcad
```

6. Ověřte, že jsou služba Client Acceptor a agent správně nastaveni:
   a. Přihlaste se ke vzdálenému systému.
   b. Pomocí webového prohlížeče se připojte k systému HOST1 pomocí této adresy a portu:

```
http://HOST1.xyz.yourcompany.com:1581
```

Windows Ruční konfigurace uzly serveru proxy pro připojení na vzdáleném systému Windows

Postupujte takto, abyste přidali uzel serveru proxy pro připojení do vzdáleného systému Windows. Tato úloha se vyžaduje, když chcete přidat druhý uzel serveru proxy pro připojení systému Windows do vašeho prostředí.

Než začnete

Než budete pokračovat s touto úlohou, ujistěte se, že je nakonfigurován primární uzel systému Windows uzel serveru proxy pro připojení.

Informace o této úloze

Postupujte takto na vzdáleném systému Windows serveru proxy pro připojení:

Postup

1. Nainstalujte následující produkty na vzdáleném systému Windows serveru proxy pro připojení:
   - zotavení
   - modul pro přesouvání dat produktu IBM Spectrum Protect

   Přistupujte k oběma produktům pomocí obrazu produktu IBM Spectrum Protect for Virtual Environments ke stažení. Podrobné instalační pokyny jsou k dispozici ve znalostním centru IBM v tématu
   “Instalace komponent Data Protection for VMware na systémech Windows” na stránce 21
2. Získejte obsah souboru ukázkových voleb z uzlu serveru proxy pro připojení systému Windows, který byl vytvořen, a přidejte jej do souboru voleb na vzdáleném systému Windows serveru proxy pro připojení:
   a) Na primárním systému Windows serveru proxy pro připojení přejděte do okna **Konfigurace** v grafickém rozhraní produktu Data Protection for VMware vSphere.
   b) Klepněte na volbu **Upravit konfiguraci TSM** v seznamu **Úlohy**. Načtení zápisníku konfigurace může chvíli trvat.
   c) Přejděte na stránku **Dvojice uzlů serverů proxy pro připojení** a klepněte na volbu **Přidat dvojici serverů proxy pro připojení**.
   d) V tabulce ve sloupci Primární uzel přejděte na uzel serveru proxy pro připojení systému Windows s nevyřízeným umístěním a klepněte na volbu **Nová nastavení**.
   e) Poznamenejte si hesla **primárního uzlu** a **partnerského uzlu Linux**. Tento panel můžete použít k úpravě nebo vytvoření vhodného hesla.
   f) Zkopírujte obsah ukázkového souboru `dsm.opt`, který je zobrazen v dialogovém okně **Nastavení serveru proxy pro připojení**.
   g) Vložte nebo přidejte obsah ukázkového souboru `dsm.opt` do souboru voleb na vzdáleném systému Windows serveru proxy pro připojení. Pojmenujte soubor voleb pomocí konvence, která identifikuje jeho roli jako vzdálené uzel serveru proxy pro připojení.
   Například: `dsm.REMOTE1_MP_WIN.opt`.

Omezení: Nepovolujte volbu Bez sítě LAN (ENABLELANFREE YES) v souboru voleb. Tato volba není podporována pro uzly serveru proxy připojení.

3. Zadejte tento příkaz modulu pro přesouvání dat, chcete-li nastavit uživatele a heslo VMware pro uzel serveru proxy pro připojení:

   Tip: Chcete-li spustit příkazový řádek dsmc, otevřete nabídku **Windows Start** a vyberte volby **Programy→ IBM Spectrum Protect → Příkazový řádek klienta zálohování**.

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <administrátor> <heslo1>
   -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

4. Zadáním následujícího příkazu ověřte připojení k serveru IBM Spectrum Protect:

   ```
   dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

   Tento příkaz zobrazuje informace o vaší relaci, včetně aktuálního názvu uzlu, je-li relace zavedena, informace o serveru a informace o připojení serveru.

5. Nastavte službu CAD (Client Acceptor Service) a službu plánovače modulu pro přesouvání dat dokončením tohoto postupu:

   Tento krok používá průvodce Konfigurace grafického rozhraní klienta IBM Spectrum Protect k nastavení služby CAD a služby plánovače. Standardně se služba agenta vzdáleného klienta rovněž nastaví pomocí průvodce. Pokud pro tuto úlohu používáte obslužný program konfigurace služby klienta IBM Spectrum Protect (`dsmcutil`), ujistěte se, že máte také instalovanou službu agenta vzdáleného klienta.
   Spusťte průvodce konfigurací klienta nástroje IBM Spectrum Protect z nabídky souboru přechodem do **Nástroje >Průvodce nastavením**:

   a) Vyberte volbu `Nápověda ke konfiguraci webového klienta TSM`. Zadejte požadované informace.

      1) Ve volbě `Kdy chcete, aby se služba spustila?` vyberte `Automaticky při zavádění systému Windows`.

      2) Ve volbě `Přejete si spustit službu po dokončení tohoto průvodce?` vyberte `Ano`.

      Když je operace úspěšně dokončena, vraťte se na úvodní stránku průvodce a pokračujte na krok b.

      Tip: Pokud na stejném systému nakonfigurujete více než jeden uzel serveru proxy pro připojení, musíte pro každou instanci služby Client Acceptor uvést jinou hodnotu portu.

   b) Vyberte volbu `Nápověda ke konfiguraci plánovače klienta TSM`. Zadejte požadované informace.

      1) Při zadávání názvu plánovače se ujistěte, že vyberte volbu `Použít démona služby Client Acceptor ke správě plánovače`.

      2) Ve volbě `Kdy chcete, aby se služba spustila?` vyberte `Automaticky při zavádění systému Windows`.

      3) Ve volbě `Přejete si spustit službu po dokončení tohoto průvodce?` vyberte `Ano`.

6. Ověřte, že jsou služba Client Acceptor a agent správně nastaveni. Pomocí webového prohlížeče se připojte k systému HOST1 pomocí této adresy a portu:

   ```
   http://HOST1.xyz.yourcompany.com:1581
   ```

Windows Linux Ruční konfigurace schopností obnovy souborů na sekundárním serveru ve vzdáleném systému Windows

Můžete ručně nakonfigurovat schopnosti obnovy souborů na sekundárním serveru na vzdáleném systému Windows. K dokončení této úlohy se musíte ujistit, že jsou naimplementovány dvojice uzlů na

sekundárním serveru proxy pro připojení k obnově souborů, aby bylo možné obsloužit sekundární server IBM Spectrum Protect. Tuto úlohu lze také naimplementovat v prostředí s více doménami.

Než začnete

Oba virtuální počítače serveru proxy pro připojení Windows a Linux musí být dostupné a spuštěné. Každý sekundární server vyžaduje dvojici uzlů sekundárního serveru proxy pro připojení pro operace obnovy souborů. Každý virtuální počítač serveru proxy pro připojení musí mít také spuštěnou službu **Microsoft iSCSI Initiator Service**. Další informace naleznete v části Windows Spuštění služby Microsoft iSCSI Initiator a Linux Konfigurace dvojice uzlů serverů proxy pro připojení selže s chybou ANS3144W - Linux.

Windows Virtuální počítače serveru proxy pro připojení musí splňovat tyto předpoklady:

- Splňovat minimální hardwarové požadavky, jak je popsáno v části Hardwarové a softwarové požadavky: Data Protection for VMware
- Být členy stejné domény jako host virtuálního počítače, který má být obnoven.

  Poznámka: V prostředí více domény musí být počítače serveru proxy pro připojení členy stejné domény, kterou jsou členy uživatelé virtuálních počítačů.

Postup

1. Vytvořte dvojici uzlů serverů proxy pro připojení:
   a) Vyberte dva nové počítače serveru proxy pro připojení k pro schopnosti obnovy souborů. Podle potřeby je nainstalujte s produktem IBM Spectrum Protect.
      - Windows Během instalačního procesu vyberte volby > **Typ instalace: rozšířený** > **Pouze funkce modulu pro přesouvání dat**.
      - Linux Během instalačního procesu vyberte volbu **Modul pro přesouvání dat Data Protection for VMware**

   b) Windows
   Vytvořte server proxy pro připojení se systémem Windows:
      1) Na kartě **Modul pro přesouvání dat** vyberte volbu **Nový modul pro přesouvání dat**.
      2) Ujistěte se, že název modulu pro přesouvání dat končí řetězcem `REMOTE_MP_WIN`.

         Poznámka: Pokud se názvy modulů pro přesouvání dat Windows a Linux neshodují, nebo nekončí správným řetězcem, dvojice uzlů serverů proxy pro připojení se nevytvoří. Místo toho se považují za moduly pro přesouvání dat.
      3) Poskytněte adresu IP pro název hostitele modulu pro přesouvání dat na virtuálním počítači Windows.
      4) Poskytněte jméno uživatele a heslo služby vCenter.
      5) Klepněte na tlačítko **PŘIDAT**.

         Poznámka: Také se vytvoří nepožadovaná služba plánování. Tuto službu plánování můžete odstranit nebo ignorovat.

   c) Linux
   Vytvořte server proxy pro připojení se systémem Linux:
      1) Na kartě **Modul pro přesouvání dat** vyberte volbu **Nový modul pro přesouvání dat**.
      2) Ujistěte se, že použijete stejný název modulu pro přesouvání dat, který jste použili pro server proxy pro připojení Windows, ale tentokrát končící řetězcem `REMOTE_MP_LNX`.

         Poznámka: Pokud se názvy modulů pro přesouvání dat Windows neshodují, nebo nekončí správným řetězcem, dvojice uzlů serverů proxy pro připojení se nevytvoří. Místo toho se považují za moduly pro přesouvání dat.

3) Poskytněte adresu IP pro název hostitele modulu pro přesouvání dat na virtuálním počítači Linux.
4) Poskytněte jméno uživatele a heslo služby vCenter.
5) Klepněte na tlačítko **PŘIDAT**.
6) V příkazovém řádku spusťte tento příkaz:

```
iscsiadm -m discovery -t sendtargets -p server proxy pro připojení partnera
```

kde *server proxy pro připojení partnera* je adresa IP serveru proxy pro připojení partnera Linux.

d) Po výběru karty **Server proxy pro připojení** ověřte klepnutím na tlačítko **Aktualizovat**, že jsou zobrazeny oba servery proxy pro připojení Windows a Linux a jsou v ověřeném stavu.

2. Spusťte operaci obnovení souboru na nové dvojici uzlů serverů proxy pro připojení:

a) Na novém počítači serveru proxy pro připojení Windows upravte soubor voleb obnovy souborů:

```
C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\frConfig.props
```

Pokyny, jak upravit soubor voleb obnovy souborů, naleznete v části “Volby obnovy souboru” na stránce 47.

b) Použijte následující změny v souboru `frConfig.props`:

```
default_mp_address=LOCALHOST
default_mp_nodename=název_uzlu_nového_serveru_proxy_pro_připojení_windows
enable_filerestore=true
```

kde *název_uzlu_nového_serveru_proxy_pro_připojení_windows* uvádí název uzlu, který je přidružený k novému serveru proxy pro připojení Windows.

c) Restartujte služby na serveru proxy pro připojení restartováním webového serveru IBM Spectrum Protect for Virtual Environments.

d) Nastavte uživatele domény a heslo pro operace obnovy souborů pomocí souboru voleb, který je přidružený k novému serveru proxy pro připojení Windows, a zadáním následujících příkazů v příkazovém řádku:

```
dsmc set password –type=domain cldev1.local\frank tajný údaj -
optfile=dsm.název_uzlu_nového_serveru_proxy_pro_připojení_windows.opt
```

kde *tajný údaj* uvádí heslo a *název_uzlu_nového_serveru_proxy_pro_připojení_windows* uvádí název uzlu, který je přidružený k novému serveru proxy pro připojení Windows.

Poznámka: Ve výše uvedeném příkazu je `clidev1.local\frank` uživatel v doméně `clidev1.local`. Tento uživatel musí také být členem domény, kde se vytváří server proxy pro připojení Windows. Další informace naleznete v tématu Windows Předpoklady pro obnovu souborů.

e) Chcete-li spustit uživatelské rozhraní obnovy souborů pro tento sekundární server, zadejte následující adresu URL serveru proxy pro připojení Windows:

```
https://název_hostitele:9081/FileRestoreUI/
```

kde *název_hostitele* uvádí název hostitele serveru proxy pro připojení Windows, který je hostitelem uživatelského rozhraní obnovy souborů.

Ruční konfigurace několika služeb Client Acceptor v systému Linux

Za určitých okolností může být přínosné použití více služeb dsmcad na jediném hostiteli klienta systému Linux.

Informace o této úloze

Tato úloha nastavení několik instancí dsmcad, které se spustí automaticky při spuštění systému:

Postup

1. Vytvořte dvě jedinečné sekce uzlu v souboru dsm.sys (tento soubor se standardně nachází v `/opt/tivoli/tsm/client/ba/bin/`):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
  COMMMethod                TCPip
  TCPPort                   1500
  TCPServeraddress   localhost
  nodename           node1
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
  managedservices    webclient sched
  httpport           1581
  passwordaccess     generate

SErvername node2
  COMMMethod                TCPip
  TCPPort                   1500
  TCPServeraddress   localhost
  nodename           node2
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
  managedservices    webclient sched
  httpport           1582
  passwordaccess     generate
```

   Tip: Může být prospěšné zahrnout jisté volby zahrnutí/vyloučení, abyste odlišili tyto uzly. V opačném případě mohou být stejná data zálohována pomocí těchto dvou názvů uzlů.

2. Vytvořte dva soubory dsm.opt, jeden pro každý uzel (tyto soubory se standardně nacházejí v `/opt/tivoli/tsm/client/ba/bin`):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Povolte `passwordaccess generate` tak, že se přihlásíte pomocí pověření pro oba uzly:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Vytvořte dvě kopie výchozího skriptu inicializace `rc.dsmcad` (tento skript se standardně nachází v `/opt/tivoli/tsm/client/ba/bin`):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Upravte rc.dsmcad-node1:
   a) Změňte tento řádek pro distribuce systému Red Hat Enterprise Linux:

```
daemon $DSMCAD_BIN
```

      Na tento řádek:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

   b) Změňte tento řádek pro distribuce systému SUSE Linux Enterprise Server:

```
startproc $DSMCAD_BIN
```

      Na tento řádek:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. Upravte rc.dsmcad-node2:
   a) Změňte tento řádek pro distribuce systému Red Hat Enterprise Linux:

```
daemon $DSMCAD_BIN
```

   Na tento řádek:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

   b) Změňte tento řádek pro distribuce systému SUSE Linux Enterprise Server:

```
startproc $DSMCAD_BIN
```

   Na tento řádek:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

7. Vytvořte nové odkazy v `/etc/init.d/`, které budou ukazovat na dané dva nové skripty inicializace rc.dsmcad. Tyto odkazy umožňují službě inicializace systému Linux spustit služby dsmcad při spuštění systému:

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. Zaregistrujte dva nové skripty rc pomocí příkazu **chkconfig**:

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. Otestujte konfiguraci pomocí příkazu **service dsmcad start**, abyste se ujistili, že se skripty načtou a spustí bez problémů:

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

   Text příkazu se umístí na dva řádky v tomto příkladu, aby se pojalo formátování stránky.

10. Restartujte a potvrďte, že se dané dvě instance dsmcad automaticky spustily:

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

   Text příkazu se umístí na dva řádky v tomto příkladu, aby se pojalo formátování stránky.

Úprava konfiguračního souboru VMCLI

Konfigurační soubor VMCLI (`vmcliConfiguration.xml`) obsahuje nastavení pro komponentu Data Protection for VMware vSphere.

Instalační proces produktu Data Protection for VMware vyžaduje, aby uživatel uvedl adresu IP serveru vCenter a to, zda se má povolit přístup ke grafickému rozhraní pomocí webového prohlížeče. Nicméně po instalaci již nelze instalačním programem upravit adresu IP serveru a přístupovou metodu grafického rozhraní.

Chcete-li aktualizovat tato nastavení, můžete ručně upravit konfigurační soubor VMCLI (`vmcliConfiguration.xml`). Tento soubor se vytvoří během instalace v následujících umístěních:
Na systémech Windows:
`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI`
Na systémech Linux:
`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/`

Chcete-li upravit to, zda povolit přístup ke grafickému rozhraní pomocí webového prohlížeče, zadejte jednu z následujících hodnot do parametru **<enable_direct_start></enable_direct_start>**:

- *yes* Ke grafickému rozhraní lze přistupovat přímo pomocí webového prohlížeče. Například:

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* Ke grafickému rozhraní nelze přistupovat přímo pomocí webového prohlížeče. Například:

```
<enable_direct_start>no</enable_direct_start>
```

Chcete-li použít grafické uživatelské rozhraní pro ochranu prostředí vSphere, uveďte následující hodnotu v parametru **<mode></mode>**:

- *vcenter* Grafické rozhraní se používá k ochraně prostředí vSphere. Například:

```
<mode>vcenter</mode>
```

Chcete-li upravit adresu IP serveru vCenter, ujistěte se, že je nastaven parametr **<mode>vcenter</mode>**, poté uveďte adresu IP do parametru **<vcenter_url></vcenter_url>**. Například:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

Hodnota `https://` je vyžadována na začátku adresy IP serveru vCenter. Hodnota `/sdk` je vyžadována na konci adresy IP serveru vCenter.

Příklady souborů `vmcliConfiguration.xml`

Následující soubor `vmcliConfiguration.xml` je nakonfigurován pro ochranu prostředí vSphere a pro grafické rozhraní je povolen přístup webového prohlížeče:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
    <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
    <interruptDelay>900000</interruptDelay>
    <mode>vcenter</mode>
    <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
    <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

Dodatek B. Migrace do strategie trvale přírůstkového zálohování

Pomocí této procedury migrujte existující plány, zásady a uzly uzel modulu pro přesouvání dat zálohy pro použití ve strategii přírůstkové trvalé zálohy.

Než začnete

Můžete použít strategii trvale přírůstkové úplné zálohy, která byla implementována ve verzi produktu Data Protection for VMware 6.2 a 6.3. Chcete-li pokračovat v použití strategie trvale přírůstkové úplné zálohy, nemusíte měnit své zásady nebo plány. Musíte zajistit, že upgradujete pouze vaše uzly modulu pro přesouvání dat na verzi 6.4 (nebo novější), jak je dokumentováno v následující proceduře. Pokud však chcete použít strategii trvale přírůstkové zálohy, musíte kromě aktualizace uzlů modulu pro přesouvání dat na verzi 6.4 (nebo novější) také aktualizovat plány a zásady pro uzly modulu pro přesouvání dat, které provádějí přesun do této strategie trvale přírůstkové zálohy.

Chcete-li migrovat existující plány produktu Data Protection for VMware do strategie trvale přírůstkové zálohy, musíte dokončit úlohy zdokumentované v této proceduře.

Důležité:

- Ačkoli jsou některé úlohy diskrétní, musí být nakonec upgradovány všechny aplikace a komponenty, aby mohly plně využívat výhod strategie trvale přírůstkové zálohy. Tato příručka poskytuje všechny informace, které vás provedou jednotlivými úlohami.
- Pro dokončení úplného procesu migrace je k dispozici několik metod. Avšak metody dokumentované v této příručce jsou považovány za úsporné metody pro typická prostředí produktu Data Protection for VMware.
- Plán, který má být v této proceduře migrován, je plán vytvořený pomocí průvodce zálohou grafického rozhraní produktu Data Protection for VMware vSphere. Pokud byl plán, který se má migrovat, vytvořen ručně, musí být aktualizace plánu identifikované v této proceduře také provedeny ručně.

Informace o této úloze

Postup

1. Upgradujte všechny záložní servery vStorage, které chrání jednotlivý nástroj vCenter. Ujistěte se, že je tento upgrade dokončen ve stejný čas pro všechny uzly modulu pro přesouvání data.
   - Tento upgrade vyžaduje instalaci modulu pro přesouvání dat produktu IBM Spectrum Protect verze 6.4 (nebo novější) na záložním serveru vStorage.
   - Jako oddělená úloha nemusíte dokončit Krok 2 nebo Krok 3 okamžitě po Kroku 1. Po upgradování uzlů modulu pro přesouvání dat můžete pokračovat v zálohování virtuálních počítačů ve vašem existujícím prostředí. Krok 2 a Krok 3 můžete dokončit, když je k dispozici užitečnější příležitost.

   Tip: Pokud vaše prostředí používá více záložních serverů vStorage, zvažte upgradování pouze jednoho serveru. Pak před upgradováním zbývajících záložních serverů vStorage ověřte, že váš server úspěšně funguje.
2. Aktualizujte zásady zálohování a plány zálohování, aby implementovaly trvale přírůstkové zálohování:

   Dokončete následující úlohy zásady zálohy na serveru IBM Spectrum Protect zadáním příkazů v klientovi administrativního příkazového řádku (`dsmadmc`):

   a. Vytvořte třídu správy pro odpovídající doménu a sadu zásad pro vaše trvale přírůstkové zálohy. Tento příklad vytvoří třídu správy `mgmt_ifincr28` pro doménu `domain1` a sadu zásad

prodbackups. Název třídy správy je použit k popisu strategie trvale přírůstkové zálohy, která zachovává 28 verzí zálohy:

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Zachovat 28 verzí zálohy"
```

b. Vytvořte záložní skupinu kopií pro vaše trvale přírůstkové zálohy. Tento příklad vytvoří standardní záložní skupinu kopií pro doménu domain1, sadu zásad prodbackups a třídu správymgmt_ifincr28:

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

Položky standard type=backup jsou výchozími hodnotami a jejich uvedení není požadováno. Jsou v tomto příkladu zahrnuty pro ilustraci, že název skupiny kopií je STANDARD, a že typ skupiny kopií je backup (místo archive).

c. Aktualizujte záložní skupinu kopií pomocí odpovídajících nastavení verze, uchování a vypršení platnosti:

Zapamatujte si: V produktu Data Protection for VMware verze 6.2 a 6.3 jsou verze zálohy, uchování a vypršení platnosti založeny na úrovni granularity řetězce zálohy. Tato metoda znamená, že přestože je provedena trvale přírůstková úplná i přírůstková záloha (jako součást strategie trvale přírůstkové úplné zálohy 6.2 a 6.3), počítá vypršení platnosti verze pouze úplné zálohy. V produktu Data Protection for VMware verze 6.4 (nebo novější) jsou verze zálohy, uchování a vypršení platnosti založeny na úrovni granularity řetězce jednotlivé zálohy. Tato metoda znamená, že vypršení platnosti verze počítá trvale přírůstkové úplné i přírůstkové zálohy.

Parametr verexists uvádí maximální počet verzí zálohy virtuálního počítače, které se mají uchovat na serveru. Pokud operace trvale přírůstkové zálohy způsobí překročení tohoto počtu, ukončí server platnost nejstarší verze zálohy existující v úložišti serveru. Tento příklad uvádí verexists=28. Tato hodnota znamená, že je na serveru uchováno maximálně 28 verzí zálohy virtuálního počítače.

Parametr retextra uvádí maximální počet dní pro uchování verze zálohy virtuálního počítače, když se tato verze stane neaktivní. Tento příklad uvádí retextra=nolimit. Tato hodnota znamená, že je maximální počet neaktivních verzí zálohy virtuálního počítače zachován po dobu neurčitou. Avšak když je uvedena hodnota verexists, je hodnota nolimit potlačena hodnotou verexists. Jako výsledek je v tomto příkladu na serveru uchováno maximálně 28 neaktivních verzí zálohy virtuálního počítače.

Na základě nastavení popsaných v tomto kroku je záložní skupina kopií aktualizována takto:

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

V tomto příkladu se existující prostředí produktu Data Protection for VMware verze 6.3 skládá z těchto hostitelů a plánů:

- Klastr ESX (esxcluster) obsahující dva hostitele ESX (esxhost1, esxhost2).
- Plán bup_esxcluster_full spouští týdenní trvale přírůstkovou úplnou zálohu každého hostitele ESX s uzlem modulu pro přesouvání dat dm1.
- Plán bup_esxcluster_incr spouští denní trvale přírůstkovou zálohu každého hostitele ESX s uzlem modulu pro přesouvání dat dm2.

Proveďte následující úlohy plánu zálohy v grafickém rozhraní produktu Data Protection for VMware vSphere:

a. Klepnutím na ikonu v okně Řešení a aplikace klienta nástroje vSphere spusťte grafické rozhraní produktu Data Protection for VMware vSphere.

b. V okně **Začínáme** klepněte na kartu **Záloha** a otevřete okno **Správa plánů zálohy**.

c. Vyhledejte plán zálohy (použitý pro trvale přírůstkové úplné nebo přírůstkové zálohy), který se má aktualizovat. V této proceduře se použije trvale přírůstkový úplný plán `bup_esxcluster_full`.

d. Klepněte pravým tlačítkem myši na plán a vyberte volbu **Vlastnosti**.

e. Přejděte na stránku **Plán** a v rozevíracím seznamu **Strategie zálohy** uveďte **Přírůstková**.

f. Klepnutím na tlačítko **OK** uložíte aktualizaci.

g. Vyhledejte plán zálohy použitý pro trvale přírůstkové zálohy. Klepněte pravým tlačítkem myši na plán a vyberte volbu **Odstranit**. Protože byl trvale přírůstkový úplný plán `bup_esxcluster_full` aktualizován na trvale přírůstkový, není tento trvale přírůstkový plán již potřebný.

3. Nyní, když máte plán trvale přírůstkové zálohy, můžete zmenšit počet uzlů modulu pro přesouvání dat jejich sloučením:

   Tento příklad sloučí dva uzly modulu pro přesouvání dat do jednoho uzlu modulu pro přesouvání dat.

   a) Na záložním severu vStorage otevřete příkazový řádek a přejděte do adresáře, ve kterém je umístěn soubor voleb pro `dm1`.

   b) Pomocí textového editoru (jako je např. Notepad) aktualizujte tento soubor následujícími volbami:

      1) Uveďte volbu `vmmaxparallel`, chcete-li řídit počet virtuálních počítačů zálohovaných `dm1` v jednom okamžiku:

         ```
         vmmaxparallel=2
         ```

         Výchozí hodnota a minimální hodnota jsou 1. Maximální hodnota je 50.

         Tip: Pro každý uzel modulu pro přesouvání dat, který odeberete, zvyšte hodnotu `vmmaxparallel` o 1.

         Alternativně můžete uvést volbu `vmlimitperhost`, chcete-li řídit počet virtuálních počítačů zálohovaných `dm1` v jednom okamžiku ze stejného hostitele ESX:

         ```
         vmlimitperhost=1
         ```

         Tato volba je užitečná, když chcete zabránit přetížení hostitele. Výchozí hodnota je 0 (bez omezení). Minimální hodnota je 1. Maximální hodnota je 50.

   c) Přihlaste se na server IBM Spectrum Protect. Použijte klienta administrativního příkazového řádku (`dsmadmc`) a uveďte maximální počet souběžných relací zálohy virtuálního počítače, které se mohou připojit k serveru. Například:

      ```
      maxsessions=4
      ```

      Výchozí hodnota je 25. Minimální hodnota je 2.

4. Ověřte řádnou funkčnost aktualizovaných uzlů modulu pro přesouvání dat:

   a) Klepnutím na ikonu v okně Řešení a aplikace klienta nástroje vSphere spusťte grafické rozhraní produktu Data Protection for VMware vSphere.

   b) V okně **Začínáme** klepněte na kartu **Konfigurace** a zobrazte stránku **Stav konfigurace**.

   c) Na stránce **Stav konfigurace** vyberte nástroj vCenter chráněný v Kroku 1. Klepněte na uzel modulu pro přesouvání dat a zobrazte informace o jeho stavu v podokně **Podrobnosti o stavu**.

      Když zobrazuje uzel varování nebo chybu, klepněte na něj a použijte informace v podokně **Podrobnosti o stavu** k vyřešení problému. Pak vyberte uzel a klepnutím na volbu **Ověřit vybraný uzel** ověřte, zda je problém vyřešen. Klepnutím na volbu Obnovit resetujte všechny uzly.

Výsledky

Po úspěšném dokončení každé úlohy je prostředí připraveno k použití ve strategii trvale přírůstkové zálohy.

Omezení: Po migraci plánů z typů trvale přírůstkové úplné zálohy do typů trvale přírůstkové zálohy si buďte vědomi následujících omezení:

- Změna migrovaných plánů zpět do typů trvale přírůstkové úplné zálohy na virtuální počítač (souborový prostor) není podporována.
- Použití starší verze modulu pro přesouvání dat produktu IBM Spectrum Protect na migrovaném souborovém prostoru není podporováno.
- Když souborový prostor obsahuje jednu (nebo více) trvale přírůstkových záloh, není trvale přírůstková úplná záloha podporována.

Příklad řízení verze pomocí parametru `verexists`

V tomto příkladu plánu migrace používá produkt Data Protection for VMware verze 6.3 následující dva plány zálohy:

- `-mode=full`: Je naplánována týdenní trvale přírůstková úplná záloha (neděle) a maximální počet verzí zálohy virtuálního počítače pro uchování na serveru jsou čtyři (`verexists=4`).
- `-mode=incr`: Je naplánována trvale přírůstková záloha ve všední dny (pondělí až sobota).

Počet záloh provedených pro čtyřtýdenní období je 28:

- 4 trvale přírůstkové úplné zálohy (jedna týdenní úplná záloha násobená čtyřmi týdny)
- 24 trvale přírůstkových záloh (šest přírůstkových záloh ve všední dny násobených čtyřmi týdny)

Poněvadž produkt Data Protection for VMware verze 6.3 počítá pouze úplné zálohy, zachová hodnota `verexists=4` všech 28 záloh.

Chcete-li poskytnout stejnou úroveň ochrany pomocí produktu Data Protection for VMware verze 6.4 (nebo novější) a strategie trvale přírůstkové zálohy, vytvořte následující plán:
`-mode=iffull`: Je naplánována denní trvale přírůstková úplná záloha a parametr `verexists` je nastaven na 28.
Počet záloh provedených pro čtyřtýdenní období je 28:

- 1 trvale přírůstková úplná záloha (počáteční záloha vynásobená jedním dnem)
- 27 trvale přírůstkových záloh (denní přírůstkové trvalé zálohy vynásobené 27 dny)

Protože produkt Data Protection for VMware verze 6.4 (nebo novější) počítá trvale přírůstkové úplné i přírůstkové zálohy, při hodnotě `verexists=28` se zachová všech 28 záloh.

Dodatek C. Funkce usnadnění přístupu pro řadu produktů IBM Spectrum Protect

Funkce usnadnění přístupu pomáhají uživatelům s určitým postižením, například s omezenou hybností nebo vadami zraku, aby mohli úspěšně používat služby informačních technologií.

Přehled

Řada produktů IBM Spectrum Protect zahrnuje tyto hlavní funkce usnadnění přístupu:

- Práce pouze pomocí klávesnice.
- Operace, které používají čtecí zařízení obrazovky.

Řada produktů IBM Spectrum Protect používá nejnovější standard W3C, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), aby byla zajištěna shoda se standardy US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) a Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Výhody funkcí usnadnění přístupu využijete, pokud budete používat nejnovější vydání čtecího zařízení obrazovky a nejnovější webový prohlížeč, který je podporovaný produktem.

Dokumentace k produktu v Centru znalostí IBM je uzpůsobená usnadnění přístupu. Funkce usnadnění přístupu Centra znalostí IBM popisuje sekce Usnadnění přístupu v nápovědě Centra znalostí IBM (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navigace pomocí klávesnice

Tento produkt používá standardní navigační klávesy.

Informace o rozhraní

Uživatelská rozhraní nemají obsah, který bliká 2 - 55krát za sekundu.

Webová uživatelská rozhraní požadují šablony stylů CSS, aby se obsah řádně vykreslil a poskytl použitelné prostředí. Aplikace nabízí uživatelům se zhoršeným zrakem rovnocenný způsob použití systémového nastavení zobrazení, včetně vysoce kontrastního režimu. Velikost písma můžete ovládat pomocí nastavení zařízení nebo webového prohlížeče.

Webová uživatelská rozhraní zahrnují navigační orientační body WAI-ARIA, které můžete použít k rychlé navigaci do funkčních oblastí v aplikaci.

Software dodavatelů

Řada produktů IBM Spectrum Protect zahrnuje určitý software dodavatele, který nepodléhá licenční smlouvě IBM. IBM neposkytuje žádné informace o funkcích usnadnění přístupu těchto produktů. Obraťte se na dodavatele, máte-li zájem o informace o usnadnění přístupu k těmto produktům.

Související informace o usnadnění přístupu

Kromě standardního střediska podpory a webů podpory IBM má IBM rovněž telefonní službu TTY umožňující neslyšícím nebo špatně slyšícím uživatelům přístup ke službám podpory a prodeje:

Služba TTY
800-IBM-3383 (800-426-3383)
(v Severní Americe)

Informace o závazcích IBM týkajících se usnadnění přístupu naleznete na webu IBM Accessibility (www.ibm.com/able).

Upozornění

Tyto informace jsou určeny pro produkty a služby nabízené ve Spojených státech. IBM může tyto materiály poskytovat v jiných jazycích. Může však požadovat, abyste vlastnili kopii produktu nebo verzi produktu v tomto jazyce, abyste k nim měli přístup.

IBM nemusí produkty, služby nebo funkce popsané v tomto dokumentu nabízet v jiných zemích. Informace o produktech a službách, které jsou momentálně dostupné ve vaší oblasti, získáte od místního zástupce společnosti IBM. Žádný z odkazů na produkty, programové vybavení nebo služby IBM neznamená, ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program nebo služba 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 od jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Držení tohoto dokumentu vám neuděluje žádnou licenci na tyto patenty. Dotazy ohledně licencí můžete odesílat v písemné formě na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

S licenčními dotazy, které se týkají informací o dvoubajtových znakových sadách (DBCS), se obracejte na oddělení duševního vlastnictví společnosti IBM ve své zemi nebo odešlete písemný dotaz na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAK, JAK JE (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Některé jurisdikce neumožňují popření odpovědnosti za výslovné či implicitní záruky v určitých transakcích, proto se na vás toto prohlášení nemusí vztahovat.

Tyto informace mohou obsahovat technické nepřesnosti nebo typografické chyby. Zde uvedené informace se pravidelně mění; tyto změny budou začleněny do nových vydání této publikace. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiné než IBM jsou poskytovány pouze pro pohodlí uživatelů a nelze je nikterak považovat za doporučení těchto webových stránek. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

Společnost IBM může využívat nebo distribuovat libovolné informace, které jí poskytnete, jakýmkoli způsobem, který uzná za vhodný, aniž by vám proto byla jakkoli zavázána.

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119

Armonk, NY 10504-1785
USA

Tyto informace mohou být dostupné za příslušných podmínek, které v některých případech zahrnují úhradu poplatku.

Licencovaný program popsaný v tomto dokumentu a všechny pro něj dostupné licencované materiály jsou IBM poskytovány za podmínek základní smlouvy ICA (IBM Customer Agreement), Mezinárodní licenční smlouvy IBM na programy, nebo jakékoli rovnocenné smlouvy.

Data o výkonu zmiňovaná v tomto dokumentu jsou odvozená za specifických provozních podmínek. Skutečné výsledky mohou být jiné.

Informace týkající se produktů jiných společností než IBM byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM tyto produkty netestovala a nemůže potvrdit jejich přesnost, kompatibilitu nebo jiná tvrzení, která se k produktům jiných společností než IBM vztahují. Otázky týkající se možností produktů jiných společností než IBM adresujte dodavatelům těchto produktů.

Tyto údaje obsahují příklady dat a sestav používaných v každodenních obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob, společností, značek a produktů. Všechna tato jména jsou fiktivní a jejich podobnost se jmény a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly důkladně otestovány za všech podmínek. Společnost IBM proto nemůže zaručit nebo vyvodit spolehlivost, provozuschopnost a funkčnost těchto programů. Ukázkové programy jsou poskytovány "JAK JSOU", bez záruky jakéhokoli druhu. IBM nenese odpovědnost za žádné škody vzniklé ve spojení s Vaším užíváním ukázkových programů.

Každá kopie nebo část těchto vzorových programů nebo jakákoliv odvozená práce musí zahrnovat níže uvedenou copyrightovou výhradu: © (název společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů IBM Corp. © Copyright IBM Corp. _zadejte rok nebo roky_.

Ochranné známky

IBM, logo IBM a ibm.com jsou ochranné známky nebo registrované ochranné známky společnosti International Business Machines Corp., registrované v mnoha jurisdikcích po celém světě. Další názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností. Aktuální seznam ochranných známek IBM je dostupný na webu v části "Copyright and trademark information" na adrese www.ibm.com/legal/copytrade.shtml.

Adobe je registrovaná ochranná známka společnosti Adobe Systems Incorporated ve Spojených státech a případně v dalších jiných zemích.

Linear Tape-Open, LTO a Ultrium jsou ochranné známky společnosti HP, IBM Corp. and Quantum ve Spojených státech a dalších zemích.

Intel a Itanium jsou ochranné známky nebo registrované ochranné známky společnosti Intel Corporation nebo jejích poboček ve Spojených státech a dalších zemích.

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

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

Java a všechny ochranné známky založené na termínu Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.

UNIX je registrovaná ochranná známka společnosti The Open Group ve Spojených státech a dalších zemích.

VMware, VMware vCenter Server a VMware vSphere jsou ochranné známky nebo registrované ochranné známky společnosti VMware, Inc. nebo jejích dceřiných společností ve Spojených státech a případně v jiných jurisdikcích.

Podmínky pro dokumentaci k produktu

Oprávnění pro použití těchto příruček je uděleno na základě následujících podmínek.

Použitelnost
Tyto podmínky platí společně s podmínkami pro použití pro webové servery IBM.

Osobní použití
Tyto příručky můžete používat pro své osobní, nekomerční použití za předpokladu, že budou zachována všechna vlastnická práva. Nejste oprávněni distribuovat, zobrazovat nebo pořizovat odvozené práce z těchto publikací nebo jakékoli jejich části bez výslovného souhlasu společnosti IBM.

Komerční využití
Jste oprávněni kopírovat, distribuovat a zobrazovat tyto publikace výlučně v rámci vašeho podniku za předpokladu, že budou zachována všechna vlastnická práva. Nejste oprávněni pořizovat odvozené práce z těchto publikací nebo reprodukovat, distribuovat a zobrazovat tyto publikace nebo jakékoli jejich části mimo váš podnik bez výslovného souhlasu společnosti IBM.

Práva
Žádná další povolení, licence nebo práva, s výjimkou těch, která jsou výslovně udělena v tomto povolení, nejsou udělena, výslovně nebo odvozeně, k publikacím ani jiným informacím, datům, softwaru nebo jinému intelektuálnímu vlastnictví zde obsaženému.

IBM si vyhrazuje právo odebrat oprávnění zde udělené kdykoliv, podle vlastního uvážení, pokud použití publikací poškozuje vlastní zájmy nebo, jak určí společnost IBM, výše uvedené pokyny nebyly správně následovány.

Nesmíte stahovat, exportovat nebo zpětně exportovat tyto informace, pokud tak nečiníte v plném souhlasu s platnými zákony a předpisy, včetně všech zákonů a nařízení ve Spojených státech.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU NA OBSAH TĚCHTO PUBLIKACÍ. PUBLIKACE JSOU POSKYTOVÁNY "JAK JSOU", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ - NIKOLI VŠAK POUZE - ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL.

Posouzení zásad ochrany osobních údajů

Softwarové produkty IBM, včetně modelu SaaS, (“Nabídky softwaru”) mohou používat soubory cookie nebo jiné technologie ke shromažďování informací o využití produktu za účelem zdokonalení zkušenosti koncového uživatele, přizpůsobení interakcí s koncovým uživatelem nebo pro jiné účely. V mnoha případech nejsou nabídkami softwaru shromažďovány žádné osobní informace. Některé z našich nabídek softwaru vám mohou pomoci umožnit shromažďovat osobní informace. Pokud tato nabídka softwaru používá soubory cookie ke shromažďování osobních údajů, jsou specifické informace o používání souborů cookie touto nabídkou uvedeny níže.

Tato nabídka softwaru nevyužívá soubory cookie nebo jiné technologie ke shromažďování osobních údajů.

Pokud konfigurace implementované pro tuto nabídku softwaru vám jako zákazníkovi poskytují schopnost shromažďovat osobní údaje od koncových uživatelů prostřednictvím souborů cookie a jiných technologií, měli byste vyhledat vlastní právní radu týkající se zákonů použitelných pro takové shromažďování dat, včetně jakýchkoli požadavků na oznámení a souhlas.

Další informace o použití různých technologií, včetně souborů cookie, pro tyto účely naleznete na webu IBM Privacy Policy na adrese http://www.ibm.com/privacy a IBM Online Privacy Statement na adrese http://www.ibm.com/privacy/details v sekci označené “Cookies, Web Beacons and Other Technologies,” a “IBM Software Products and Software-as-a-Service Privacy Statement” na adrese http://www.ibm.com/software/info/product-privacy.

Slovníček

Je dostupný slovníček s termíny a definicemi pro řadu produktů IBM Spectrum Protect.

Viz IBM Spectrum Protect - slovníček.

Rejstřík

L

M

N

O

P

R

S

T

U

V

Z

Číslo programu: 5725-X00