Veeam Backup Server :

قلب سیستم پشتیبان گیریست به نحوی که تمامی روال ها و کارها را تعریف و اجرا می نماید. مدیریت و مانیتورینگ ماشین ها، ارتباط با vCenter ، گرفتن Snapshot ، اختصاص Backup Proxy و Storage از دیگر وظایف آن می باشد.

مراحل پروسه ی پشتیبان گیری به صورت ذیل می باشد:

۱- زمان بند یا scheduler یک پروسه یا روال کاری را شروع می نماید.

۲- سپس به vCenter متصل شده و کارها را اولویت بندی و سازماندهی می کند.

۳- فضای ذخیره سازی را بررسی می نماید.

۴- بهترین و نزدیک ترین Backup Proxy را پیدا می کند.

۵- پروسه پشتیبان گیری ماشین ها را به BP مربوطه اختصاص می دهد.

۶- آیتم های دیگر مانند پهنای باند مورد نظر برای انتقال backup را تنظیم و اختصاص می دهد.

۷- تمامی پروسه های پشتیبان گیری به ترتیب پشت سر هم یا به صورت موازی اجرا شده و در نهایت اطلاعات مربوط به backup ها و اطمینان از صحت روند کاری جمع آوری می گردد.

Proxy Server :

نقش اصلی آن پیدا کردن بهترین مسیر برای انتقال backup گرفته شده می باشد. بنا به نوع ارتباط می تواند به دو صورت ذیل باشد:

۱- ماشین فیزیکی که ارتباط مستقیم با ذخیره ساز SAN از طریق کانال فیبر نوری یا iSCSI دارد.

۲- ماشین مجازی که به فضای ذخیره ساز دسترسی دارد.

Repository :

به محل ذخیره شدن اطلاعات و backup ها می گویند و در حقیقت فولدری بر روی SAN است.

هر روند کاری یا Job تنها از یک repository می تواند استفاده کند در صورتی که هر repository می تواند به چندین job اختصاص داده شود.

Repository می تواند ویندوز یا لینوکس یا یک SMB باشد. در سیستم عامل ها باید توجه داشت که درایوهای map شده قابل استفاده نبوده و اگر نیاز به استفاده از آن ها هست، بایستی مسیر UNC و احراز هویت آن تعریف گردد. دیگر فضاهای موجود مانند دیسک های محلی و SAN متصل به سیستم عامل قابل استفاده می باشند.

اگر می خواهید از طریق WAN پروسه پشتیبان گیری را انجام دهید پیشنهاد می شود یک BP جداگانه در remote site اختصاص داده شود.

اجزای دیگر مانند Veeam Backup Enterprise Manager وجود دارند که نصب آن ها اختیاریست. VBEM در حقیقت یک اینترفیس تحت وب است که امکان مدیریت بر روی چندین Veeam backup server را می دهد. VBEM می توان بر روی سرور جداگانه و یا مشترک با backup server نصب شود.

Veeam explorer for exchange :

برای بازیابی اجزای ایمیل سرور Exchange 2010 طراحی شده است به صورتی که بتواند ایمیل های ارسالی و دریافتی و . . . را به تفکیک بازیابی کند.

Veeam explorer for sharepoint :

همانطور که از نامش پیداست، مختص پشتیبان گیری از sharepoint می باشد.

Veeam explorer for SAN Snapshot :

راه حلی اختصاصی برای ذخیره سازهای شرکت HP است تا بتوان ماشین های مجازی را به راحتی از طریق snapshot های گرفته شده توسط storage بازیابی کرد.

Veeam Backup Search :

وقتی تعداد زیادی ماشین backup گرفته شده داشته باشیم می تواند سودمند واقع گردد.

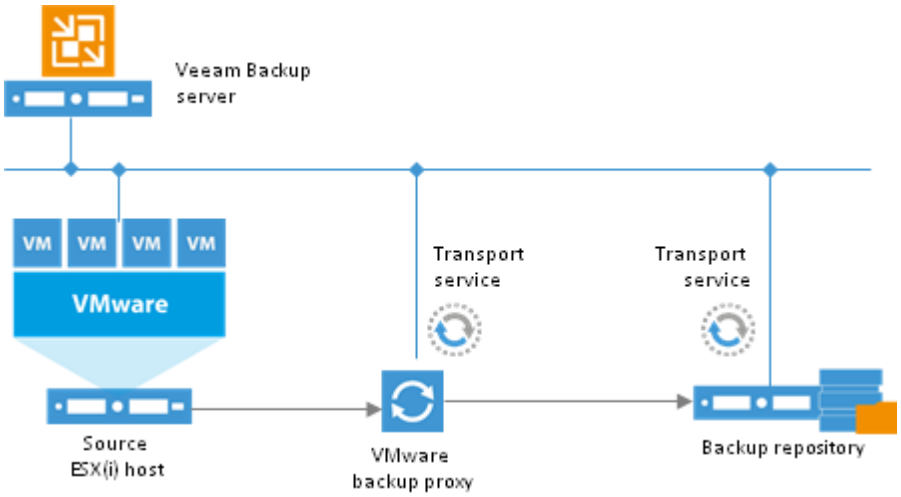
Universal Application-Item Recovery (U-AIR) :

برای بازگردانی سرویس هایی چون active directory یا SQL کاربرد دارد و نیز می تواند قسمتی از پروسه ی بازیابی را در اختیار کاربران بگذارد.

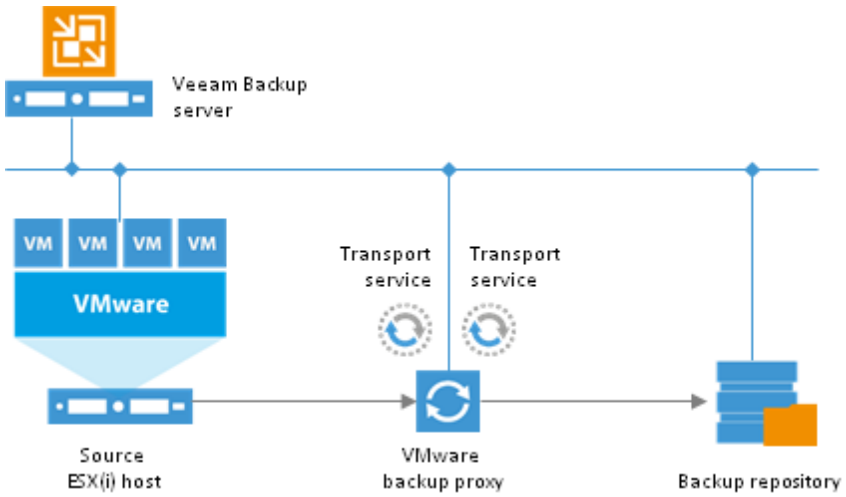
نحوه ی پشتیبان گیری در Veeam بر پایه ایجاد یک تونل بین هاست مبدا و ذخیره ساز مقصد است تا اطلاعات به صورت بلاک های پشت سر هم منتقل شوند. معمولا اولین backup به صورت full بوده و باقی به صورت incremental و فقط اعمال تغییرات می باشد.

برای پشتیبان گیری درون یک سایت، از دوسرویس یکی بر روی Source Host و دیگری بر روی Repository استفاده می شود. به سرویس اجرا شده بر روی هاست Source-side Transport Service گفته شده و سرویس اجرا شده بر روی Repository به نام Target-Side Transport Service می باشد.

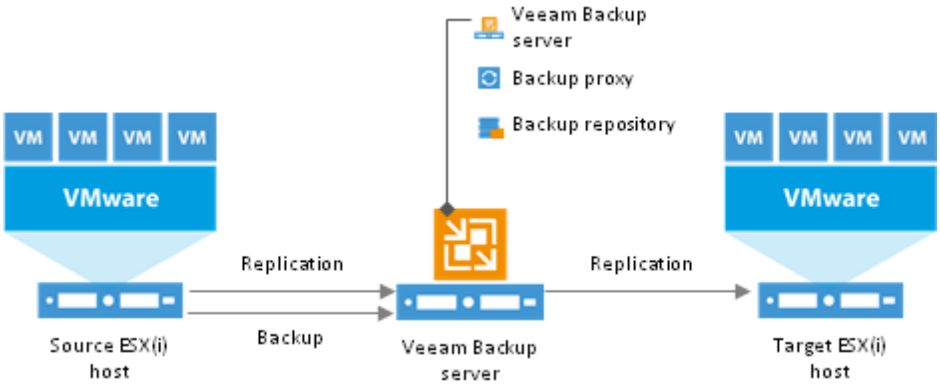
اگر Repository یک سیستم عامل ویندوزی یا لینوکسی باشد، سرویس Transport به صورت ذیل خواهد بود.



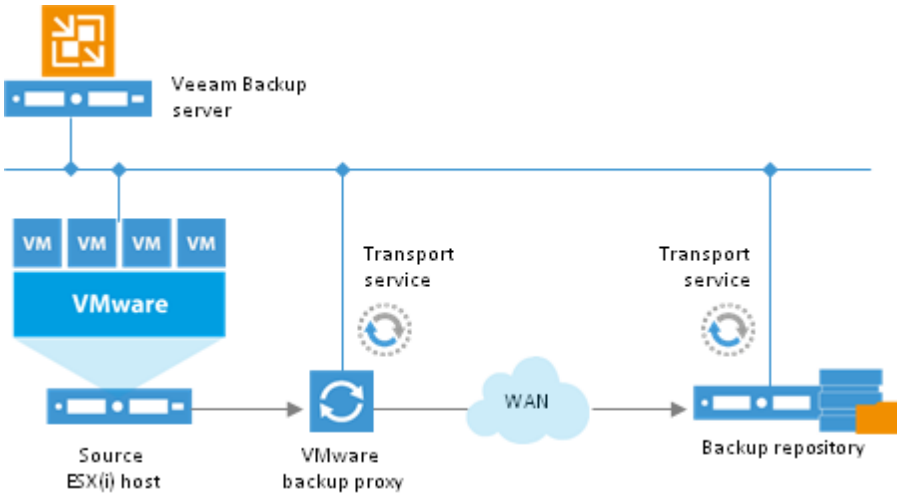
اگر Repository یک SMB باشد، سرویس Transport به صورت شکل زیر خواهد بود.



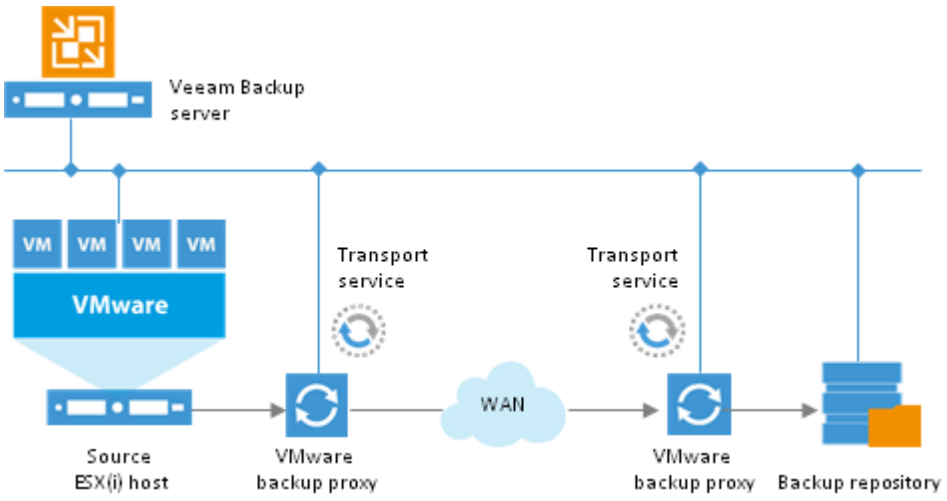
نکته: لازم به ذکر است در این حالت معمولی و ساده، می توان Veeam Backup Serverو Veeam Proxy Server و Backup Repository را بر روی یک سیستم پیاده نمود.



هنگامی که نیاز به پشتیبان گیری از طریق WAN یا لاین ارتباطی ضعیفی داشته باشیم می بایست Backup proxy را در سمت ماشین هایی که می خواهیم از آنها پشتیبان بگیریم، قرار دهیم تا سرویس Source-Side Transport را روی ان داشته باشیم. Repository هم، در طرف دیگر ارتباط قرار گرفته وسرویس Target-side Transport روی ان فعال می شود. حال با برقراری تونل ارتباطی بین این دو سرویس پروسه ی پشتیبان گیری شروع می شود.



اگر بخواهیم پشتیبان از طریق WAN را بر روی یک SMB بگیریم، باید یک backup proxy سمت ماشین ها و یکی دیگر سمت repository داشته باشیم.

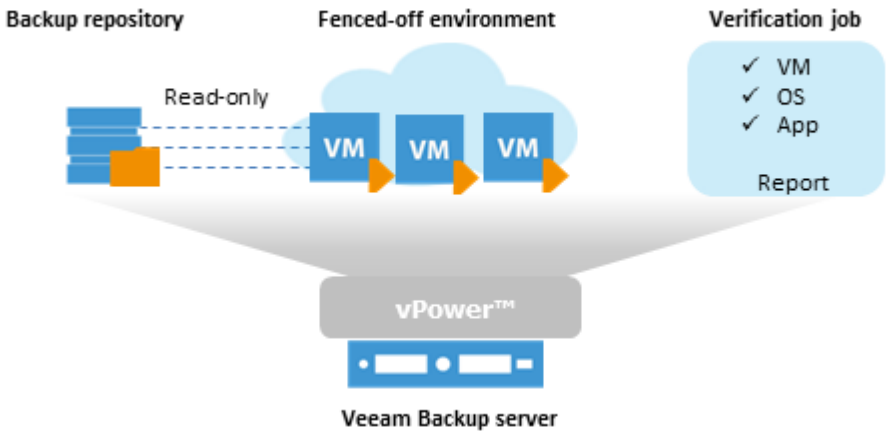


Recovery and verification : سرویس Veeam vPower بر روی ویندوز متصل به repository ،فعال بوده و به هاست ESX امکان دسترسی به backup های گرفته شده را به صورت VMDK می دهد.

SureBackup : امکان اجرای ماشین های مجازی را به صورت مستقیم از روی backup های گرفته شده در یک محیط آزمایشی می دهد.

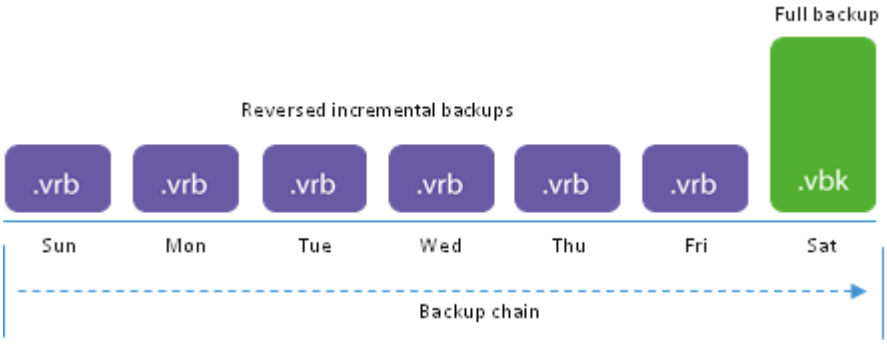
Virtual LAB : محیطی مجازی برای تست و اطمینان از صحت عملکرد ماشین های مجازی backup گرفته شده می باشد.

Recovery Verification Job : مراحل و اجزای پشتیبان گیری از قبیل سیستم عامل، ماشین مجازی و برنامه ها را برای اطمینان از صحت عملکرد بررسی می نماید.



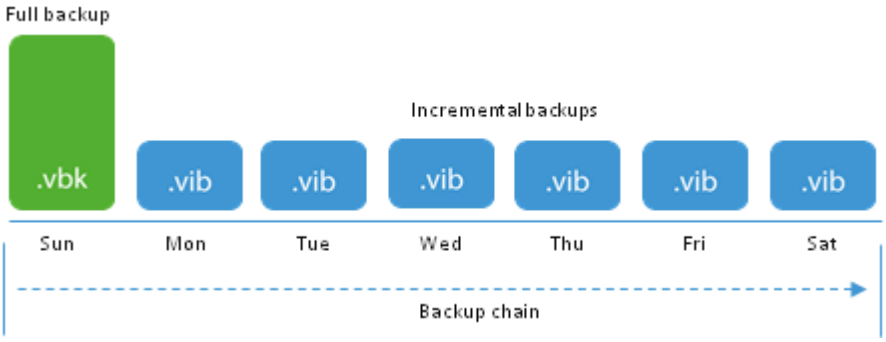
Recovery : امکان بازگردانی اطلاعات به دو صورت بر پایه image و فایل ارائه می دهد.

Reverse Incremental : پس از اولین پشتیبان گیری، تغییرات را هر دفعه به صورت بلاک های پشت سرهم گرفته و در نهایت یک Full backup با تمامی تغییرات می سازد. از این حالت برای پشتیبان گیری بر روی دیسک های محلی و ذخیره ساز استفاده می شود.



Forward Incremental :

ابتدا یک Full Backup گرفته و سپس تغییرات را گرفته و نگهداری می کند. از این روش برای پشتیبان گیری از اطلاعات یک Remote Site و یا بین ذخیره ساز ها استفاده می شود.



Backup Job :

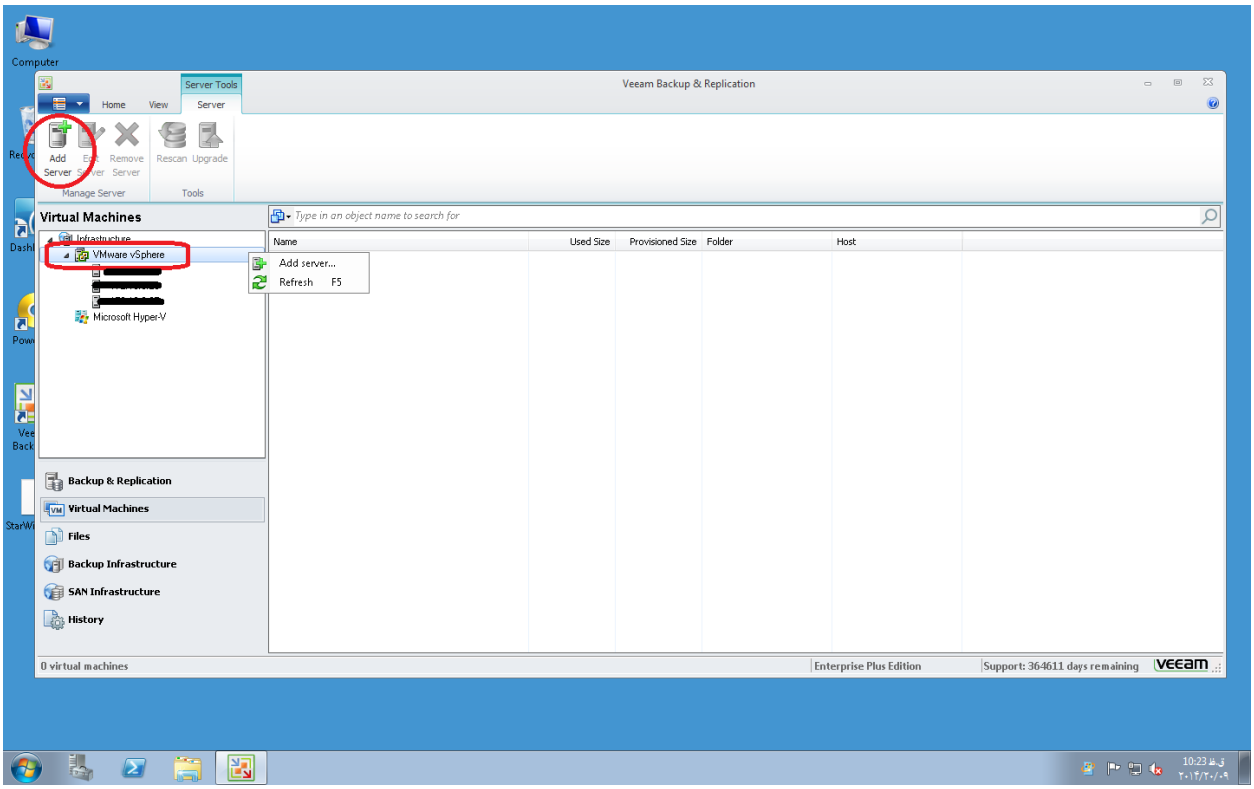
امکان ایجاد یک Duplicate backup را بر روی محل دوم یا جایی خارج از سایت می دهد.

مراحل پشتیبان گیری از ماشین های مجازی

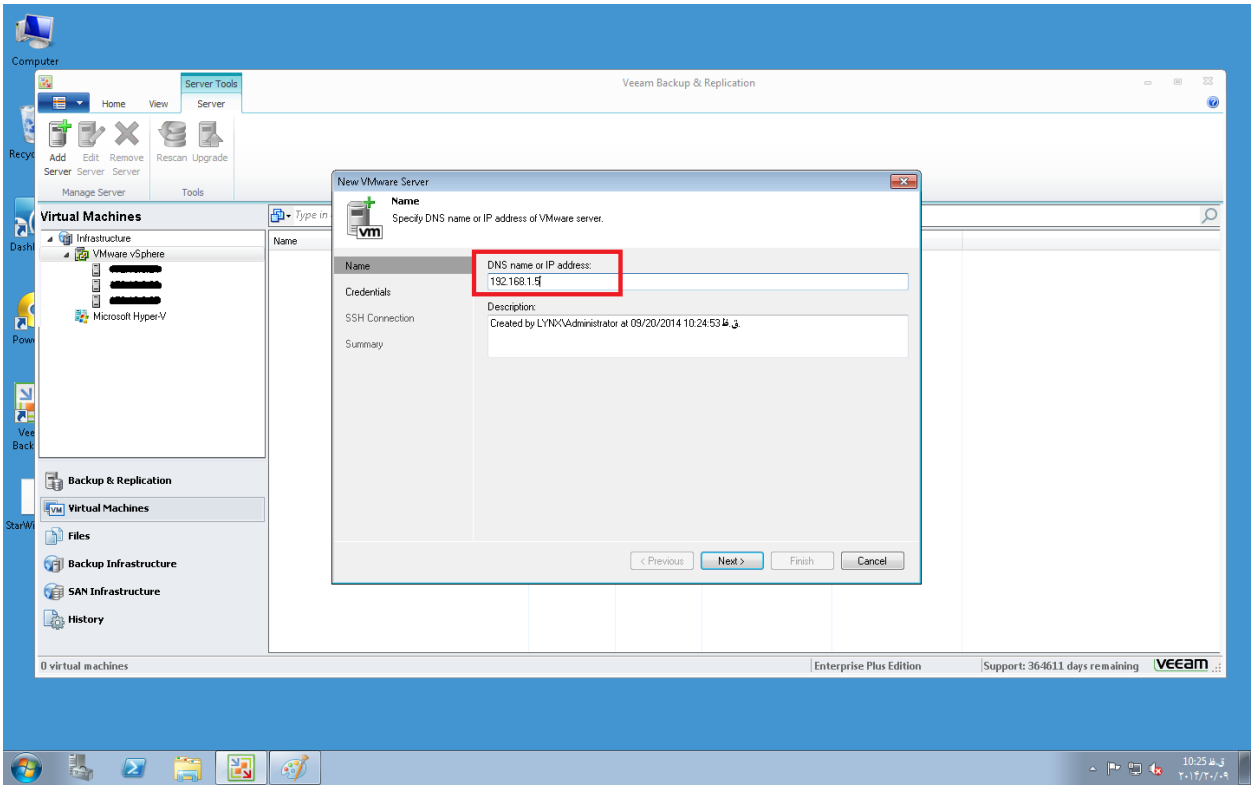
۱) اتصال به hypervisor یا vCenter

ابتدا می بایست هاست ماشین های مجازی اضافه شود تا بتوان از ماشین های مستقر بر روی آن backup گرفت. اگر چندین پلت فرم hypervisor و ماشین های فیزیکی متعدد داشتیم، بهتر است به vCenter متصل شویم تا دیگر نیازی به شناسایی تک تک هاست های موجود نداشته باشیم.

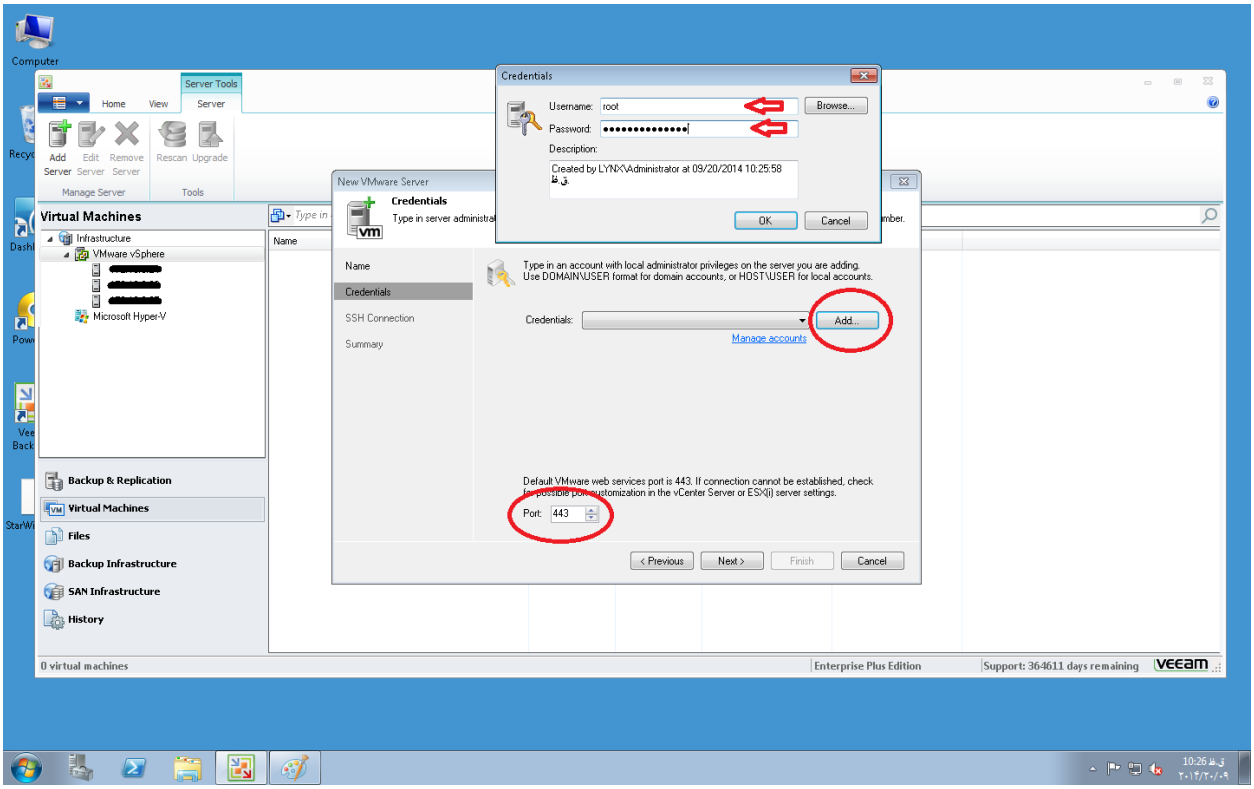
برای این کار ابتدا از مسیر زیر اقدام می نماییم:



سپس آدرس آی پی هاست مورد نظر را وارد می کنیم:



در مرحله بعد با وارد کردن نام کاربری و رمیز عبور هاست مورد نظر یا vCenter می توان به ماشین های مجازی موجود دسترسی پیدا کرد.



بایستی توجه داشت که برای الحاق vCenter از باز بودن پورت شماره ۴۴۳ اطمینان حاصل نمایید. همچنین برای هاست ESXi پورت های ۴۴۳ و ۹۰۲ و ۲۲ مورد نیاز می باشند. جدول پورت های مورد نیاز به شرح ذیل می باشند:

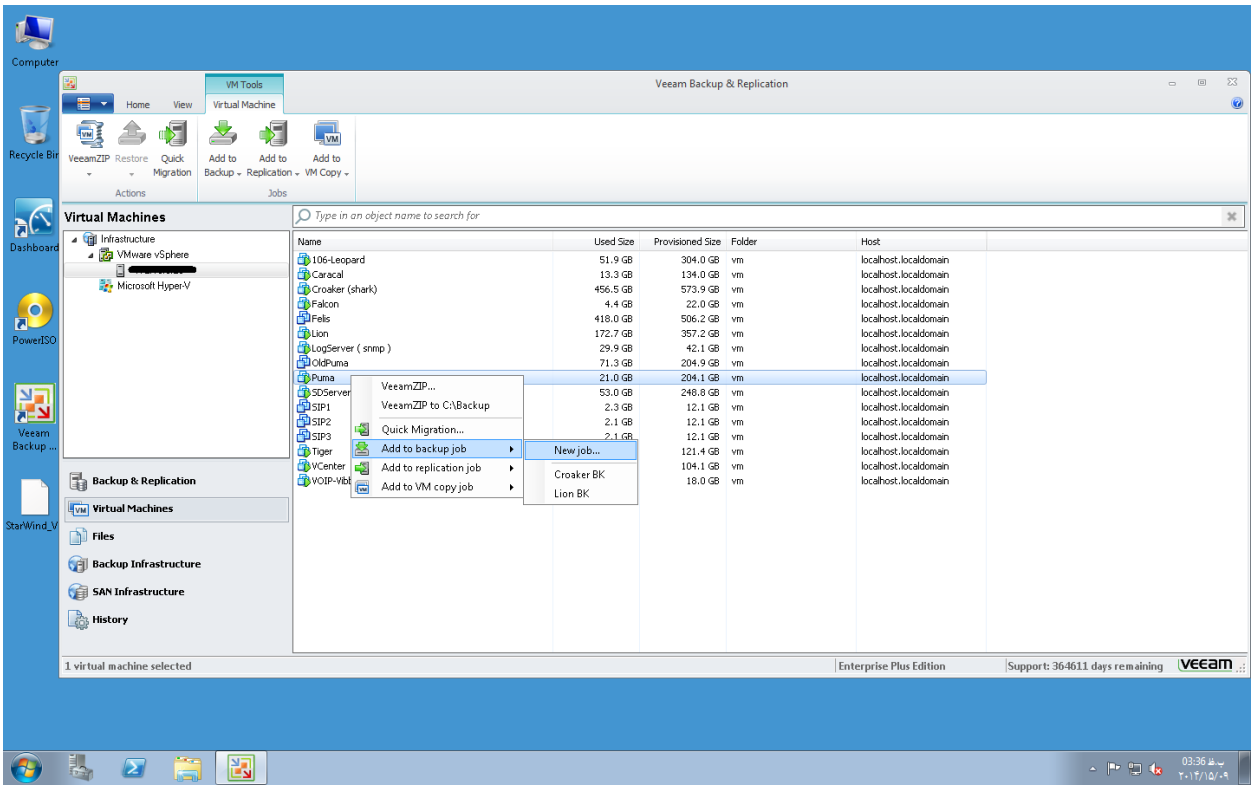
From	To	Protocol	Port	Notes
Veeam backup server	vCenter Server	HTTPS	443	Default VMware web service port that can be customized in vCenter settings
	ESX(i) server	HTTPS	443	Default VMware web service port that can be customized in ESX host settings. Not required if vCenter connection is used.
		TCP	902	VMware data mover port.
		TCP	22	Default SSH port used as a control channel, only for jobs with a full ESX target with the service console agent enabled.
	Linux server	TCP	22	Port used as a control channel from the console to the target Linux host.
	Windows server	TCP UDP	135, 137-139, 445	Ports required for deploying Veeam Backup & Replication components.
		TCP	6160	Default port used by the Veeam Installer Service.
		TCP	6162	Default port used by the Veeam Transport Service.
		TCP	6161	Default port used by the Veeam vPower NFS Service.
		TCP UDP	111 2049+ 1058+	Standard NFS ports. **Note:** If ports 2049 and 1058 are occupied, the succeeding port numbers will be used).
Linux server	Veeam backup server	TCP	2500-5000	Default range of ports used as transmission channels for jobs writing to Linux target. For every TCP connection that a job uses, one port from this range is assigned.

From	To	Protocol	Port	Notes
Communication with VMware Servers				
VMware backup proxy	vCenter server	HTTPS	443	Default VMware web service port that can be customized in vCenter settings.
	ESX(i) server	TCP	902	VMware data mover port.
		HTTPS	443	Default VMware web service port that can be customized in ESX host settings. Not required if vCenter connection is used.
Communication with Backup Repositories				
VMware backup proxy	Linux server	TCP	22	Port used as a control channel from the backup proxy to the target Linux host.
	Shared folder CIFS (SMB) share	TCP UPD	135, 137-139, 445	Ports used as a transmission channel from the backup proxy to the target CIFS (SMB) share.
Linux server	VMware backup proxy	TCP	2500-5000	Default range of ports used as transmission channels for backup jobs. For every TCP connection that a job uses, one port from this range is assigned.
Windows server	VMware backup proxy	TCP	2500-5000	Default range of ports used as transmission channels for backup jobs. For every TCP connection that a job uses, one port from this range is assigned.
Communication with Backup Proxies				
VMware backup proxy	VMware backup proxy	TCP	2500-5000	Default range of ports used as transmission channels for replication jobs. For every TCP connection that a job uses, one port from this range is assigned.

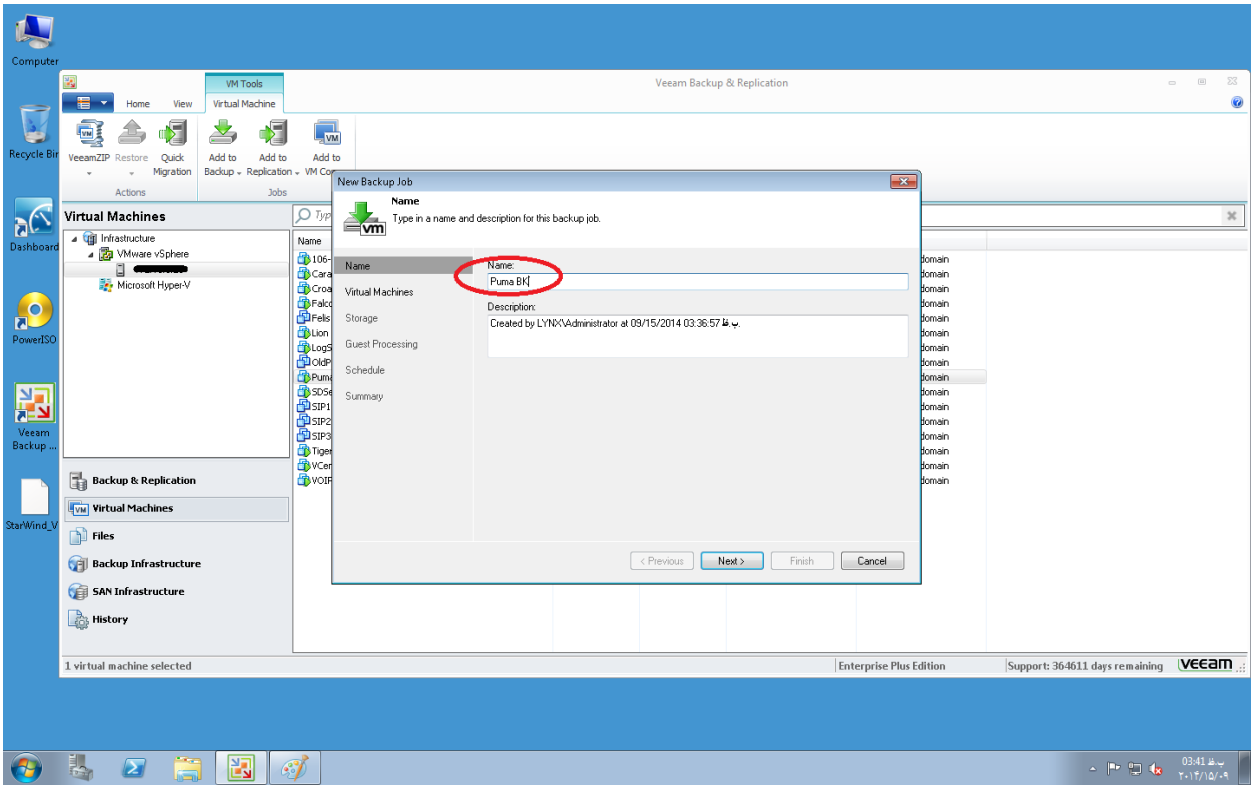
۲) پشتیبان گیری از ماشین های مجازی

مراحل ایجاد یک روند کاری برای Image گرفتن از یک یا چند ماشین مجازی به شرح زیر می باشد:

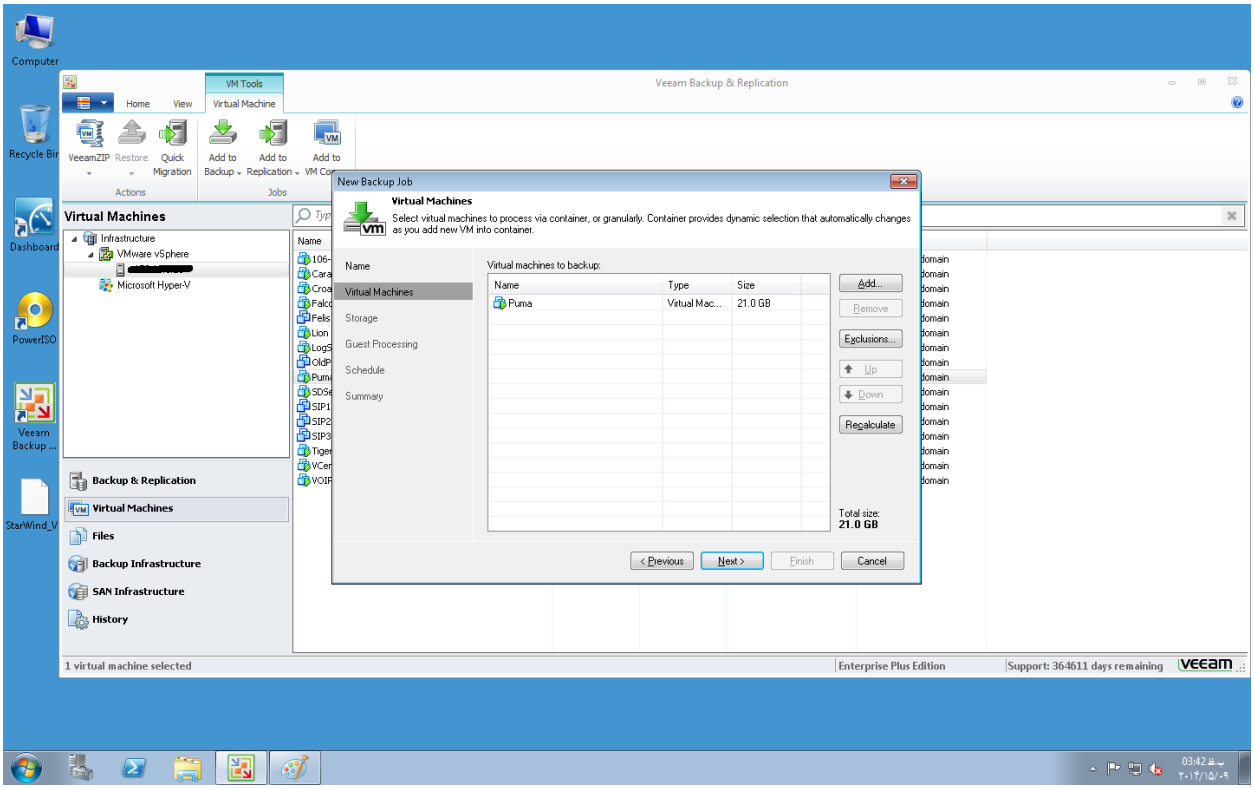
ابتدا یک روند کاری یا همان job ایجاد می کنیم.



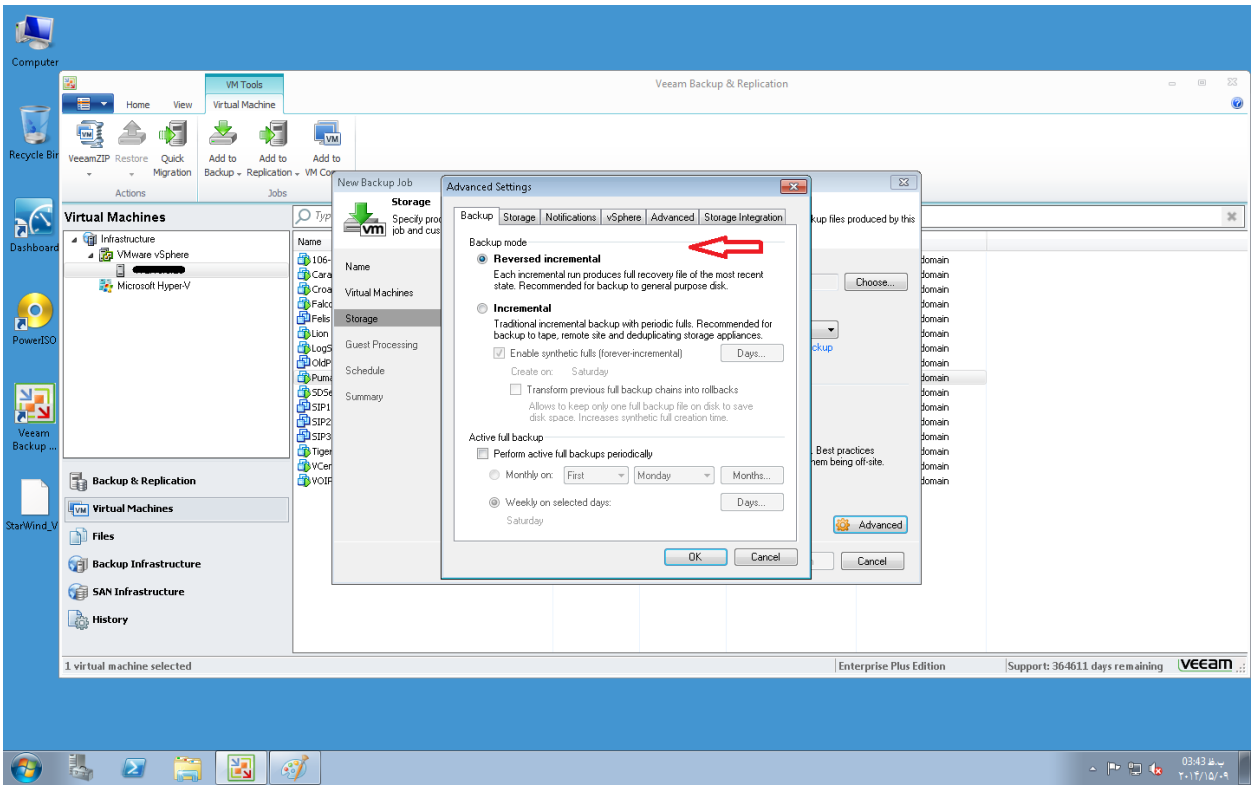
حال نام روند کاری را وارد می نماییم.



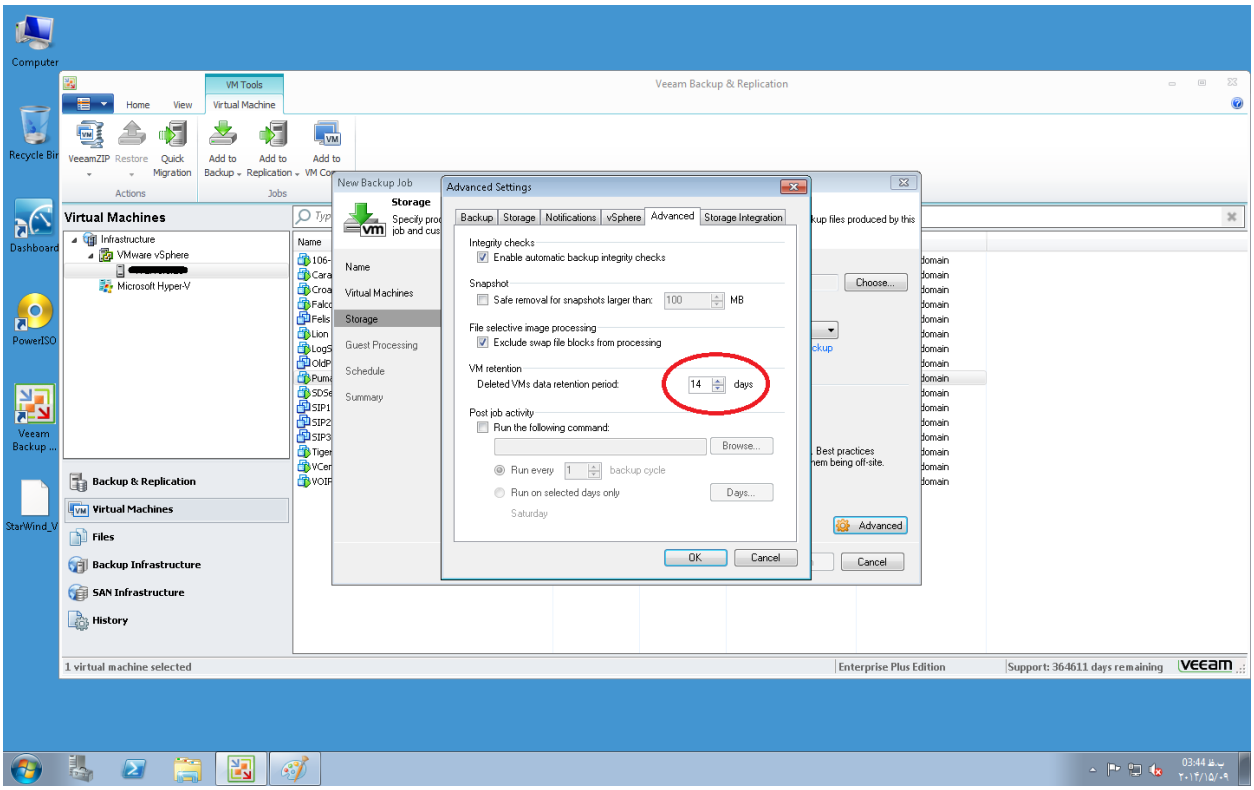
در اینجا می توان ماشین های مورد نظر را به job مربوطه اضافه نمود.



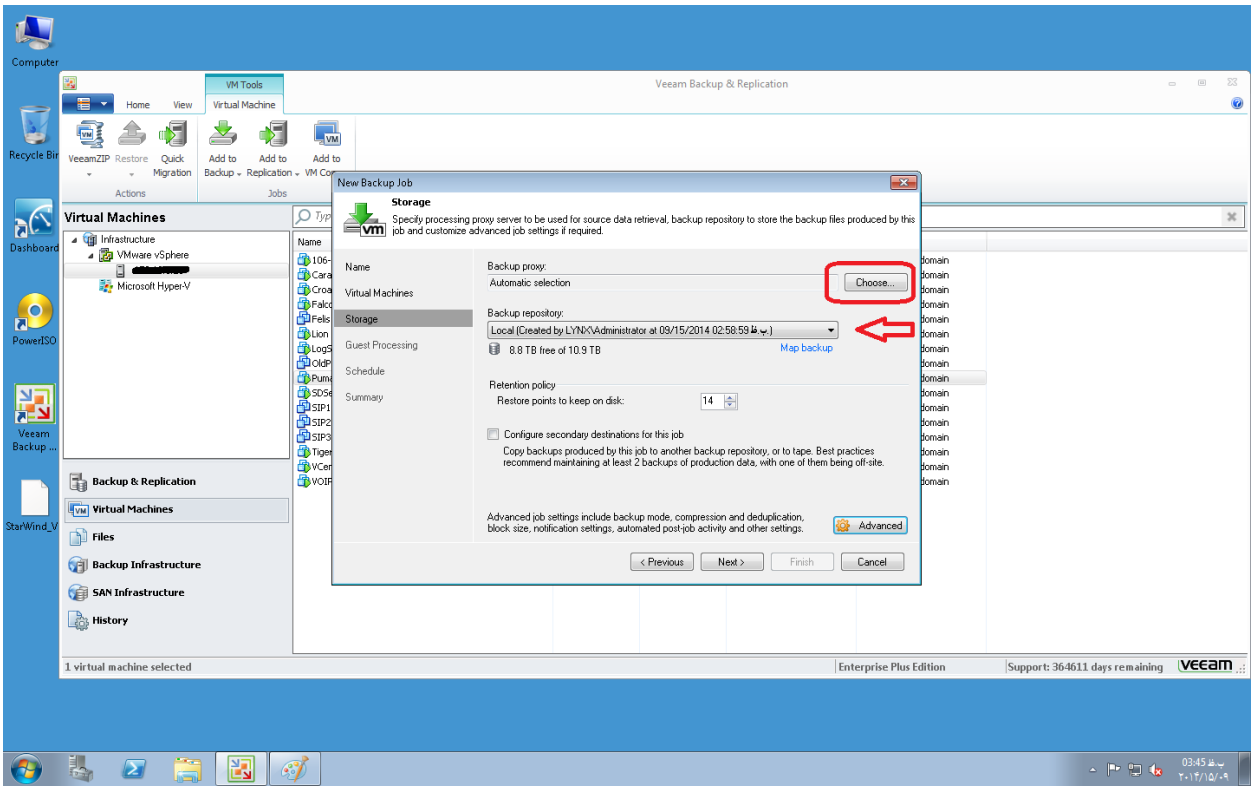
حال می توان نوع backup گیری را مشخص کرد. اگر این backup از طریق یک ارتباط WAN بود بهتر است از نوع forward incremental یا همان incremental استفاده نمود در غیر اینصورت reverse incremental می توان بهره جست.



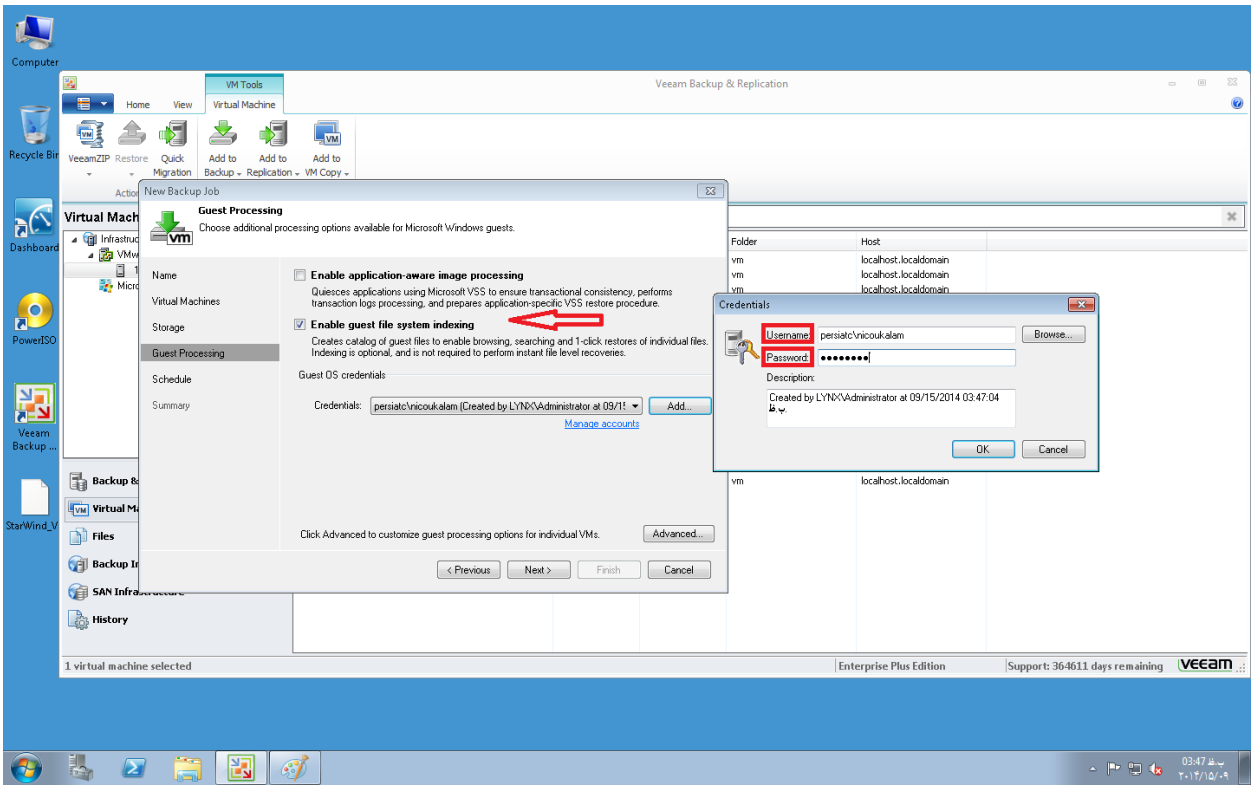
تعداد restore point های مورد نظر را می توان در قسمت VM Retention معین نمود.



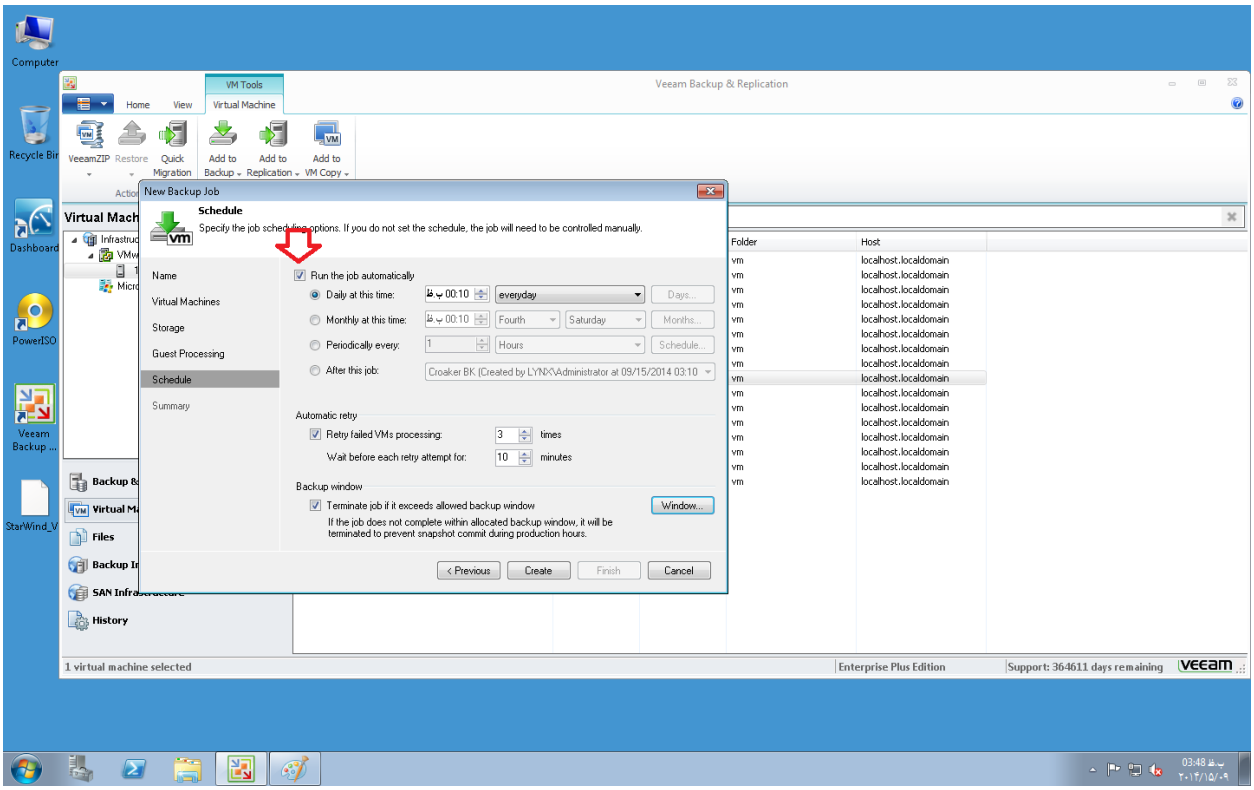
محلی که backup می خواهد در آن ذخیره شود یا همان repository را انتخاب و نیز در صورت داشتن backup proxy جداگانه، می توان مشخص نمود.



برای اتصال به ماشین مجازی لازم به نام کاربری و رمز عبور آن می باشد. همچنین اگر نیاز به index نمودن فایل های ماشین برای جستجو در آن داشته باشیم، می بایست گزینه system index را فعال کنیم.



و در آخر به زمانبندی backup گرفتن می رسیم.



نمونه ی توضیح داده شده تنها برای یک simple site بود ولی در حالت enterprise می بایست متدهای replication ، remote backup proxy و . . . پیاده سازی گردد.

محمدرضا نیکوکلام

شرکت ارتباطات پرشیا