SB C&S

Veeam × Pure Storage FlashArray
ランサムウエア対策検証レポート

2022年08月09日

第1版

SB C&S

改訂履歴

版	更新日	更新内容
第１版	2022/08/09	第１版発行

本書は、弊社にて把握、確認した内容を基に作成したものであり、利用者の環境や製品機能の仕様や動作について担保・保証するものではありません。
本書の利用に関し、トラブルが発生した場合、利用者または第三者に損害が生じた場合であっても、本書は利用者の自己責任のもと利用されているものであることを鑑み、弊社は損害賠償その他一切の責任を負いません。

本書の内容に対するテクニカルサポートは提供しておりません。

本書の記載内容は本書発行時点の情報であり、製品のバージョンアップなどによって操作手順や画面構成、機能動作などが本書記載の内容と異なることがあります。

本書に全ての記載内容は予告なく変更されることがあります。

SB C&S

目次

1. はじめに 1
1.1. 本書の目的 1
1.2. 本書の想定読者 1
2. 製品概要 2
2.1. Veeam Backup & Replication 2
2.2. Pure Storage FlashArray 2
3. 検証、あるいは作業環境 3
3.1. システム構成 3
3.2. 機器仕様 4
3.3. お客さまにてご用意いただくもの 6
3.4. 環境に関する注意点、前提条件 6
4. 事前準備 7
5. 検証の概要 8
6. 検証内容 9
6.1. 初期設定 9
6.1.1. Pure Storage Plugin のインストール手順 9
6.1.2. Veeam Console から Pure Storage を STORAGE INFRASTRUCTURE に登録する手順 12
6.1.3. 強化（書き換え不能）Linux リポジトリの登録手順 25
6.2. バックアップ 38
6.2.1. ストレージスナップショットを使用したバックアップ 39
6.2.2. スナップショットオーケストレーション 47
6.3. 強化（書き換え不能）Linux リポジトリの確認 54
6.4. SureBackup 57
6.4.1. Application Group の作成 58
6.4.2. Virtual Lab の作成 62
6.4.3. SureBackup ジョブの作成と実行 73
6.5. Secure Restore 80
6.6. SafeMode を利用したストレージスナップショットのリカバリ手順 89
7. まとめ 97
参考文献 98

1. はじめに

1.1. 本書の目的

本書は、Veeam Backup & Replication、Pure Storage FlashArray の概要説明、および 連携機能であるストレージスナップショットを使用したバックアップ、スナップショットオーケストレーション、ランサムウエア対策として Veeam Backup & Replication で利用できる強化（書き換え不能）Linux リポジトリ、SureBackup、Secure Restore、SafeMode を利用したストレージスナップショットのリカバリ手順について記載しています。

1.2. 本書の想定読者

VMware×Pure Storage FlashArray の環境に Veeam Backup & Replication を利用したランサムウエア対策を導入、および検証を実施される方を想定しています。

2. 製品概要

2.1. Veeam Backup & Replication

Veeam Backup & Replication（VBR）は、企業における、仮想、物理、クラウドベースのあらゆるワークロードに対応した包括的なデータ保護の実現を支援します。1 つのコンソールで、全てのアプリケーションおよびデータの高速で柔軟な、信頼性の高いバックアップとリストア、レプリケーションを実現します。

また、Veeam Backup & Replication V11a はランサムウエア対策として以下の機能が利用できます。

・強化（書き換え不能）Linux リポジトリ
・SureBackup
・Secure Restore

2.2. Pure Storage FlashArray

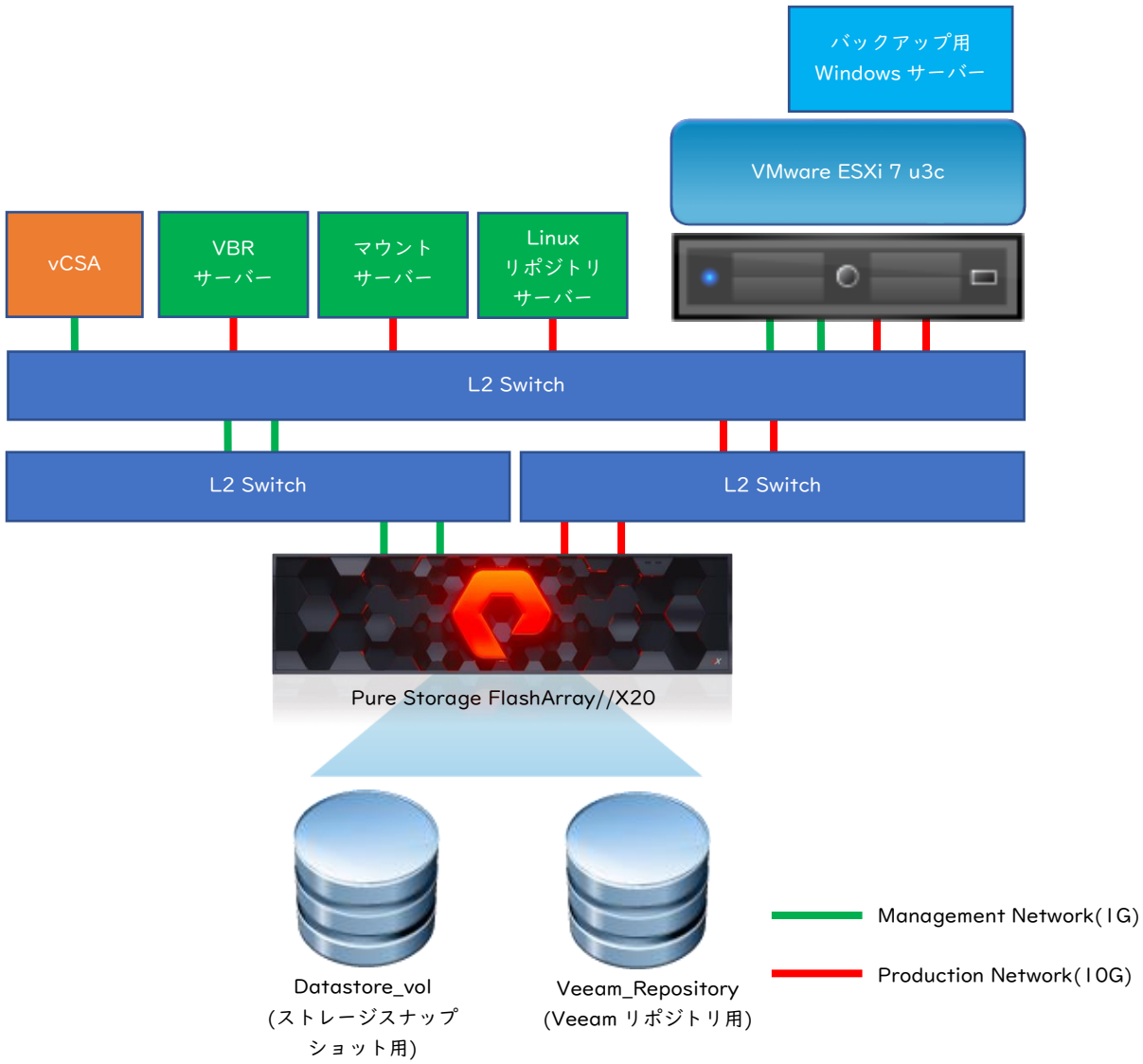
Pure Storage 社の FlashArray シリーズは、シンプルな、業界初の Tier1 向け FC/iSCSI 対応オールフラッシュ SAN ストレージです。 製品の特徴として 100%MLC フラッシュで構成されており、1ms 以下の遅延、数十万の IOPS を提供します。

また、ランサムウエア対策として SafeMode を使用することでセキュアなコピーを作成しバックアップデータとメタデータを保護します。ランサムウエアが管理者権限を持ったとしても SafeMode スナップショットの削除や変更、暗号化はできません。 わずか数回のクリックで、ビジネスクリティカルなデータの迅速かつ大規模なリストアを可能にします。 この機能は、FlashBlade、FlashArray のいずれのプラットフォームでもサポートされています。

3. 検証、あるいは作業環境

3.1. システム構成

今回の検証におけるシステム環境は以下となります。



・VBR サーバーは、Veeam Console、Backup Proxy、Gateway サーバーを兼ねています。

・マウントサーバーは、Secure Restore、SureBackup の Malware scan で使用します。

・ストレージスナップショットバックアップ用に Pure Storage より Datastore_vol を作成し ESXi のデータストアとして登録しています。
また、バックアップ保存先として、Veeam_Repository を作成し Linux リポジトリサーバーに iSCSI マウントしています。

3.2. 機器仕様

Pure Storage FlashArray

製品名	FA-X20R2
OS バージョン	Purity//FA 6.2.7
容量	960GB × 10
NIC(1 コントローラーあたり)	10/25GbE iSCSI × 2 16Gb FC × 2 10/25GbE × 2(レプリケーション用 Port) 1GbE × 2

VBR サーバー

OS バージョン	Windows Server 2019 Standard
CPU	2 × 4core
メモリ	12GB
ストレージ	ハードディスク 1：50GB ハードディスク 2：300GB
Veeam Backup & Replication バージョン	11a(11.0.1.1261 P20220302)

マウントサーバー

OS バージョン	Windows Server 2019 Standard
CPU	2 × 4core
メモリ	16GB
ストレージ	ハードディスク 1：100GB
アンチウイルスソフトウエア	Windows Defender

Linux リポジトリサーバー

OS バージョン	Ubuntu 20.04.1 LTS
CPU	2 × 4core
メモリ	32GB
ストレージ	ハードディスク 1：32GB

vCenter Server Appliance(vCSA)

バージョン	vCSA 7.0 u3c ※「デプロイサイズの選択」で、デプロイサイズ：極小とストレージサイズ：デフォルトを選択
CPU	1 × 2core
メモリ	12GB
ストレージ	579GB

ESXi01(vSphere)

バージョン	vSphere 7.0 u3c
CPU	2 × 6core
メモリ	32GB
ディスク	ディスク 1 ：300GB

Win2019-01(バックアップ用 Windows 仮想サーバー)

OS バージョン	Windows Server 2019 Standard
CPU	1×2core
メモリ	4GB
ディスク	ディスク：50GB

3.3. お客さまにてご用意いただくもの

本書の手順を実施するには、下記の環境をお客さまにてご用意していただく必要があります。

- vCenter Server Appliance(vCSA) × 1
- vSphere(ESXi) × 1
- Pure Storage FlashArray × 1
- L2 Switch × 3 (お客さまの環境に合わせてご用意ください。)
- VBR サーバー × 1
- マウントサーバー × 1
- Linux リポジトリサーバー × 1
- Windows Server(バックアップ用 Windows 仮想サーバー) × 1

3.4. 環境に関する注意点、前提条件

・今回は検証のため、基本的にデフォルト設定を使用しておりますが、実際の設定は、お客さまの環境に合わせて設定していただく必要があります。

・マウントサーバーで使用するアンチウイルスソフトウエアはデフォルトで下記 4 つの製品が定義されていますが、それ以外のアンチウイルスソフトウエアを使用する場合は、AntivirusInfos.xml ファイルに設定を追加する必要があります。

・Symantec Protection Engine
・ESET
・Windows Defender
・Kaspersky Security 10

・Pure Storage の SafeMode を有効化するには、Pure Storage サポートへ連絡が必要となります。

・本書では、検証のため Pure Storage の Eradicate 操作不可期間（24 時間～30 日）を 24 時間としていますが、本番環境で利用される場合は Eradicate 操作不可期間を十分にとっていただくことを強く推奨します。

4. 事前準備

検証環境では、事前に下記設定を実施済みです。

- VBR サーバーに Veeam Backup & Replication のインストール
- Veeam Backup & Replication の初期設定(vCenter の登録)
- Pure Storage の初期セットアップ
- Pure Storage より Volume 作成(Datasote_vol、Veeam_Repository)
- Pure Storage の SafeMode の有効化(Eradicate 操作不可期間：24 時間)
- Linux-Repository01 の iSCSI イニシエーターを構成して、Veeam_Repository を /mnt/FlashArrayVol としてマウント
- Linux-Repository01 の/mnt/FlashArrayVol に backup フォルダを作成してアクセス権の付与
- 最新の[PureStoragePlugin]を下記サイトからダウンロードして、VBR サーバーのデスクトップ上に展開
  https://www.veeam.com/download_add_packs/vmware-esx-backup/purestorage/

5. 検証の概要

以降の章より以下設定手順を記載します。

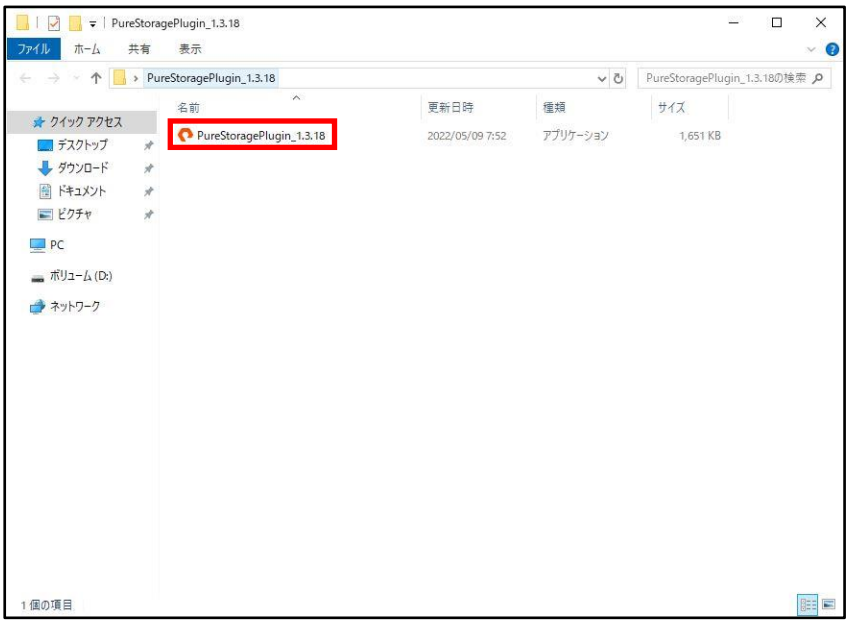
- Pure Storage Plugin のインストール手順
- Veeam Console から Pure Storage を STORAGE INFRASTRUCTURE に登録する手順
- Veeam Console から Pure Storage を Repository に登録する手順
- ストレージスナップショットを使用したバックアップ
- スナップショットオーケストレーション
- 強化（書き換え不能）Linux リポジトリの確認
- Application Group の作成
- Virtual Lab の作成
- SureBackup ジョブの作成と実行
- Secure Restore
- SafeMode を利用したストレージスナップショットのリカバリ手順

6. 検証内容

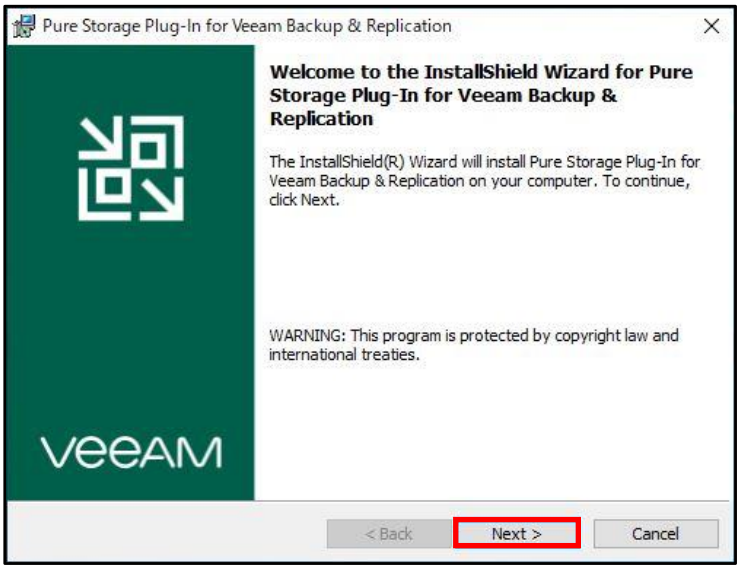
6.1. 初期設定

6.1.1. Pure Storage Plugin のインストール手順

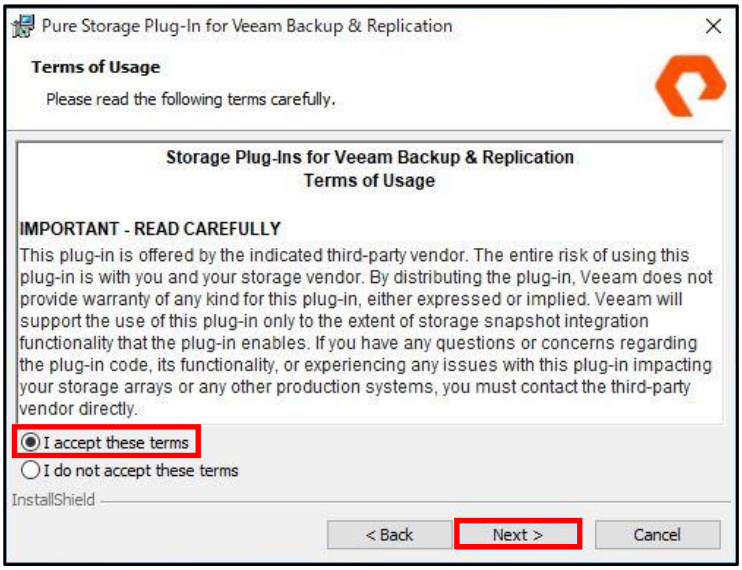
1. VBR サーバーのデスクトップに展開した[PureStoragePlugin]のインストーラーをダブルクリックします。



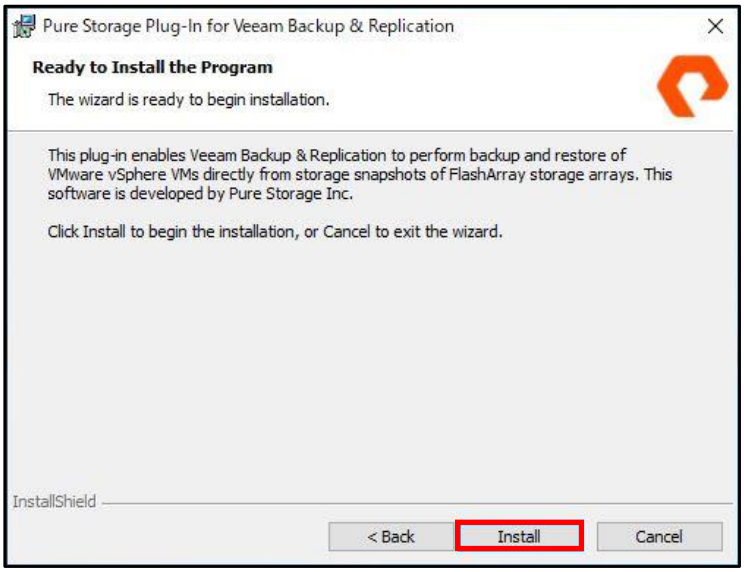
2. [Next >]をクリックします。



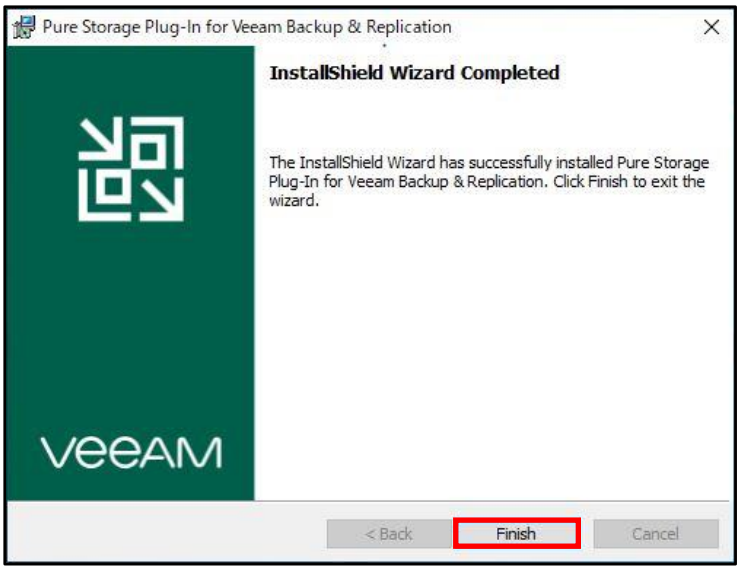
3. [I accept these terms] を選択して、 [Next >] をクリックします。



4. [Install]をクリックします。



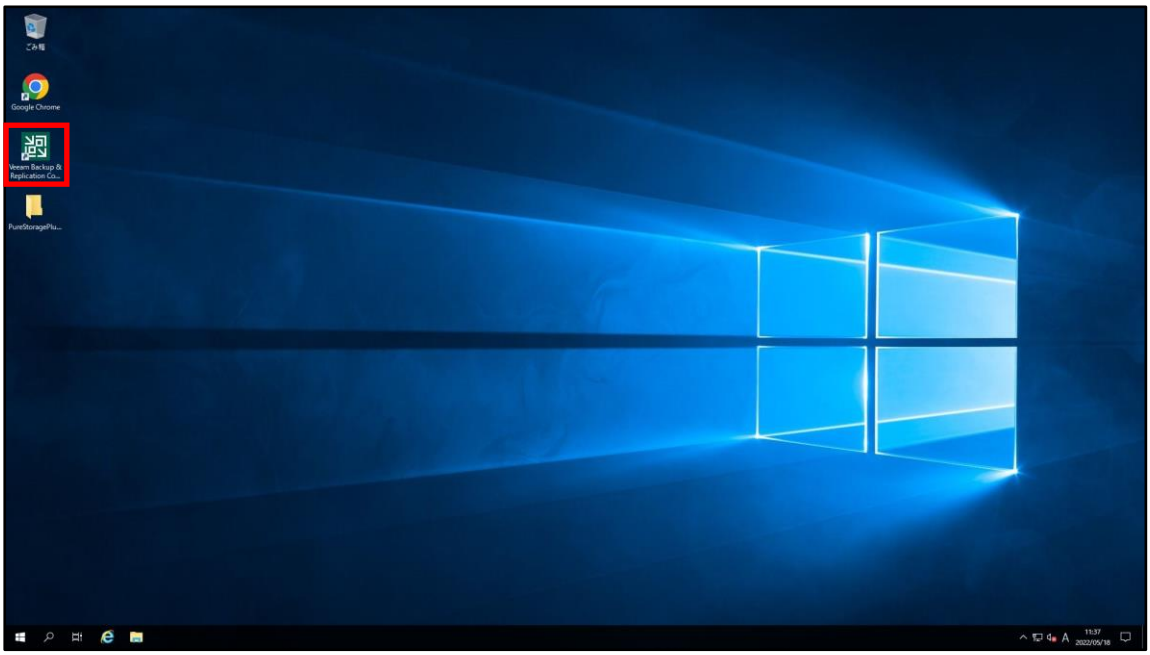
5. インストールが完了したら、[Finish]をクリックします。



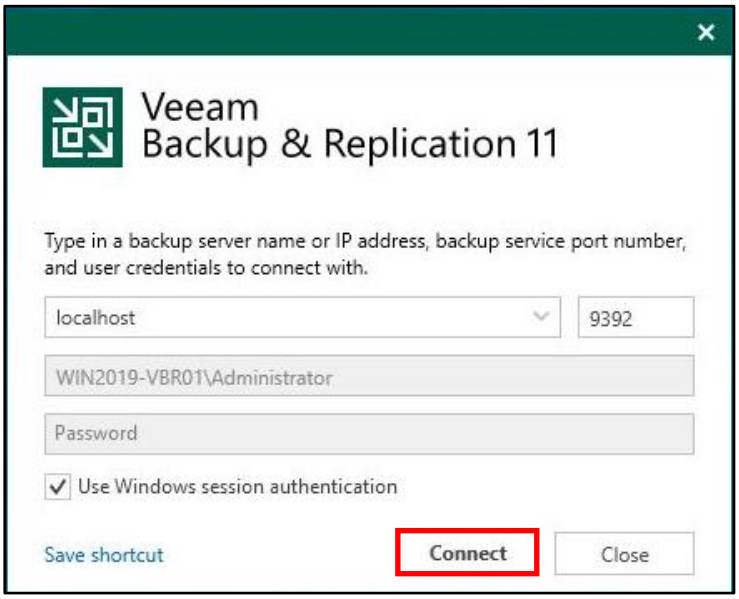
以上で Pure Storage Plugin のインストールが完了となります。

6.1.2. Veeam Console から Pure Storage を STORAGE INFRASTRUCTURE に登録する手順

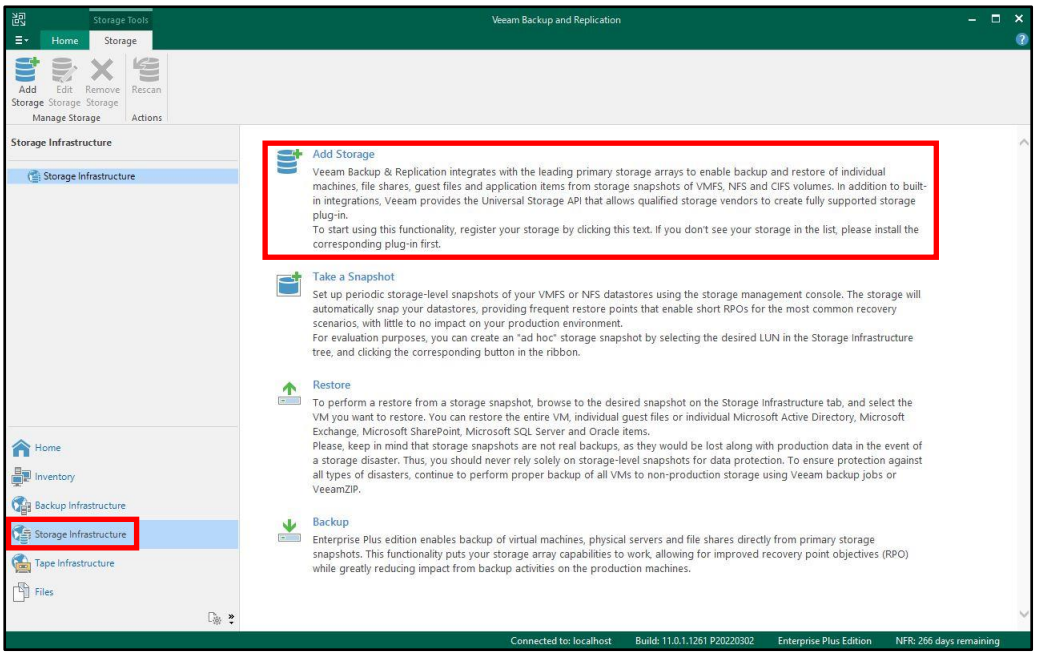
1. VBR サーバーのデスクトップ上の[Veeam Backup & Replication Console]をダブルクリックします。



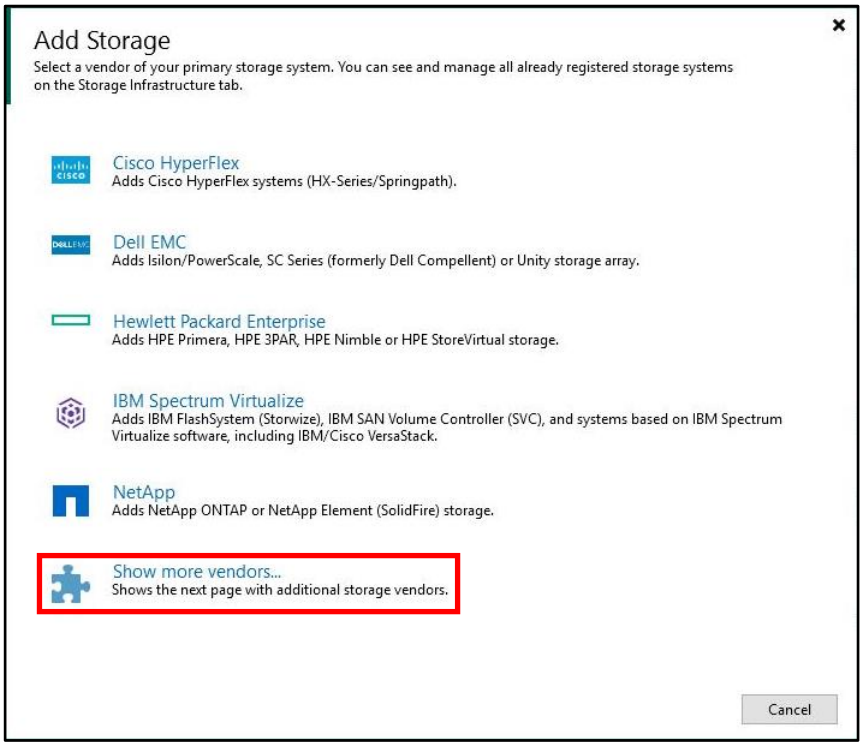
2. [Connect]をクリックします。



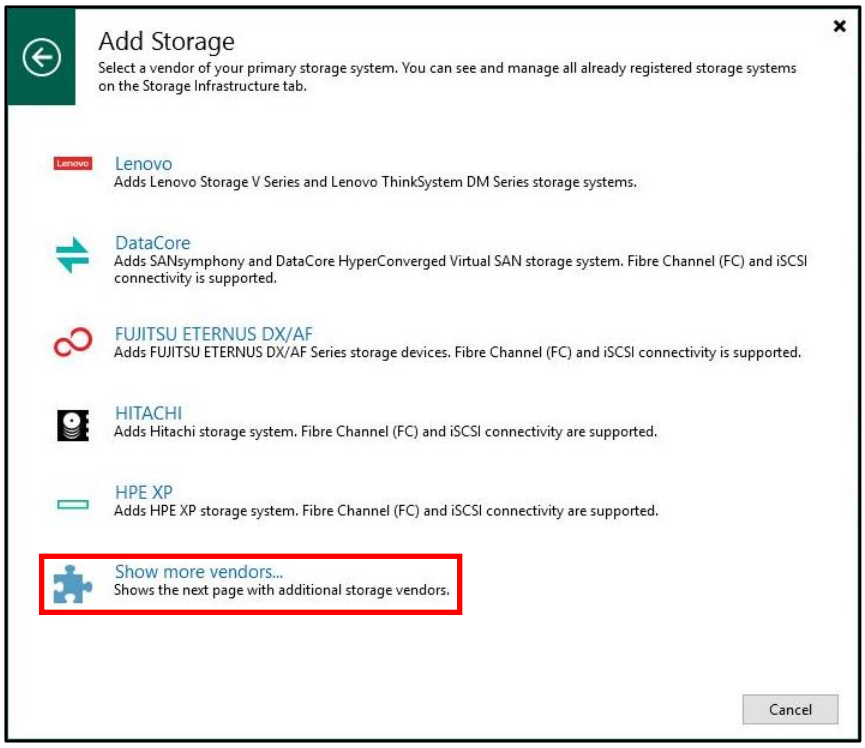
3. Veeam Backup & Replication Console の[Storage Infrastructure]-[Add Storage]をクリックします。



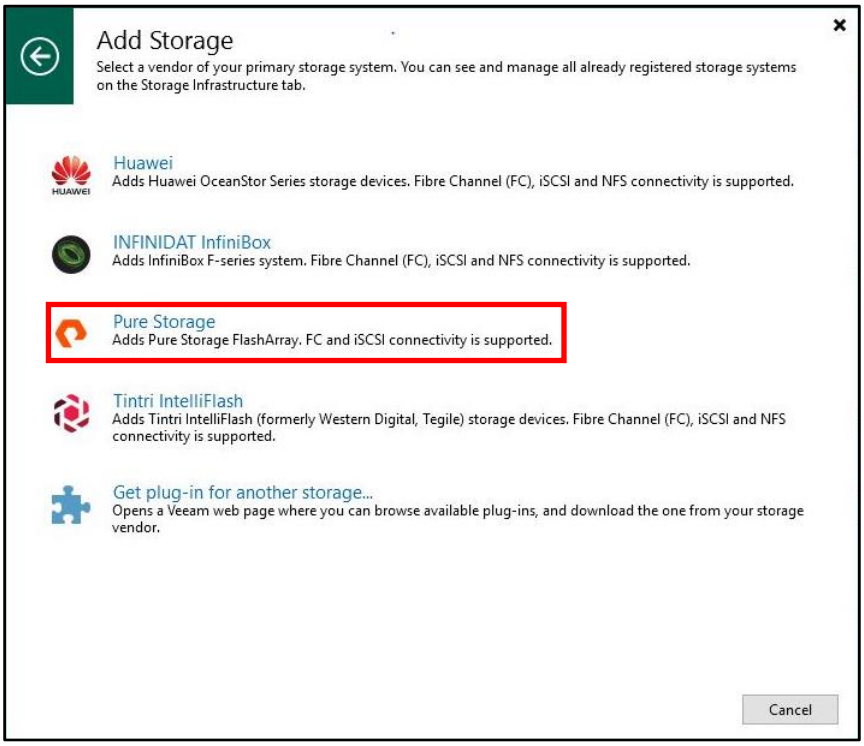
4. [Show more vendors...]をクリックします。



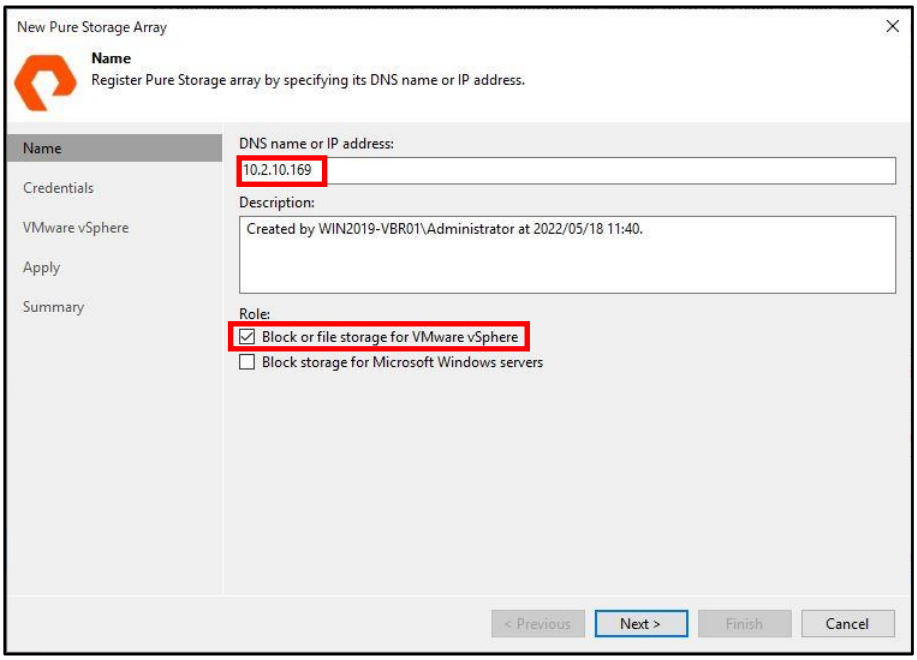
5. [Show more vendors...]をクリックします。



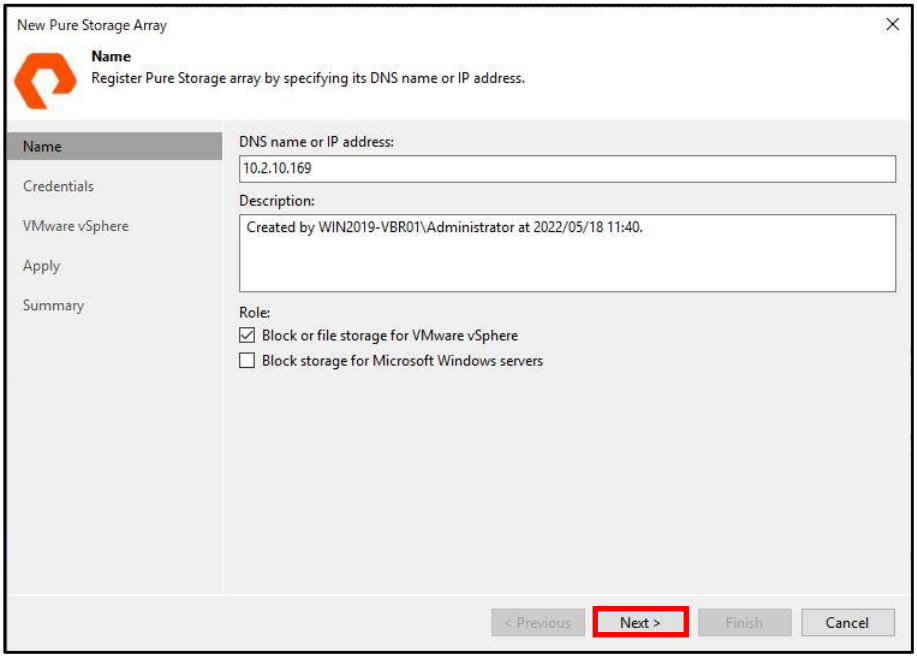
6. [Pure Storage]をクリックします。



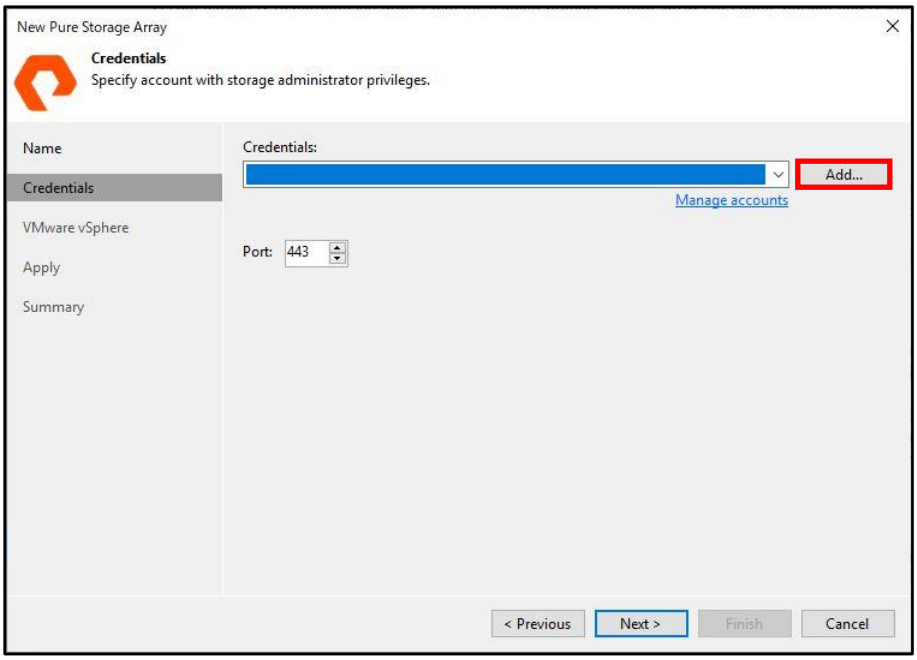
7. [DNS name or IP address:]に Pure Storage の FQDN または IP アドレスを入力して、[Block of file storage for VMware vSphere]をチェックします。



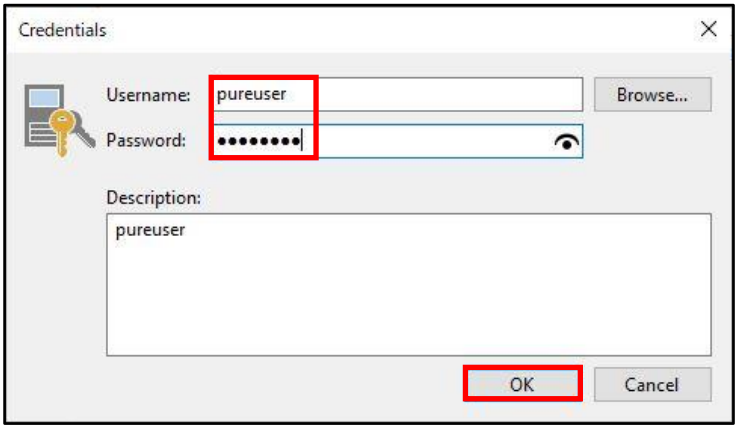
8. [Next >]をクリックします。



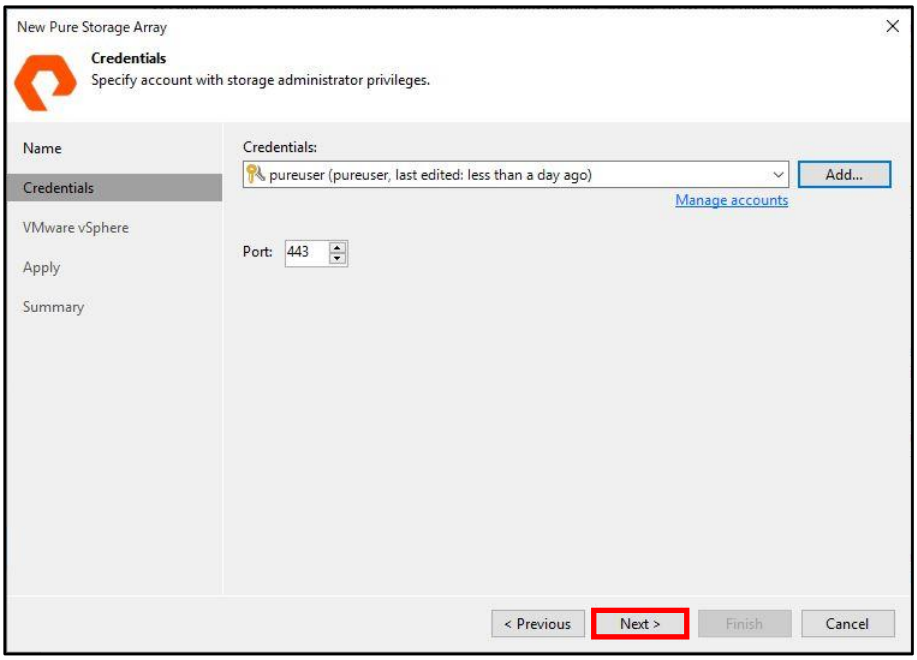
9. [Add...]をクリックします。



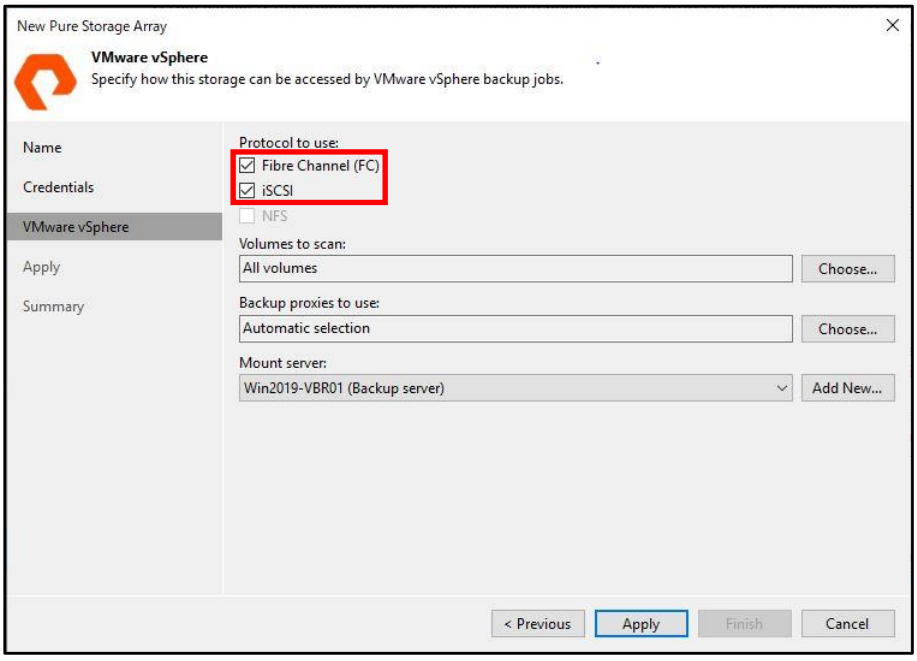
10. Pure Storage の Username と Password を入力して、[OK]をクリックします。
※本書では、[pureuser]を使用します。



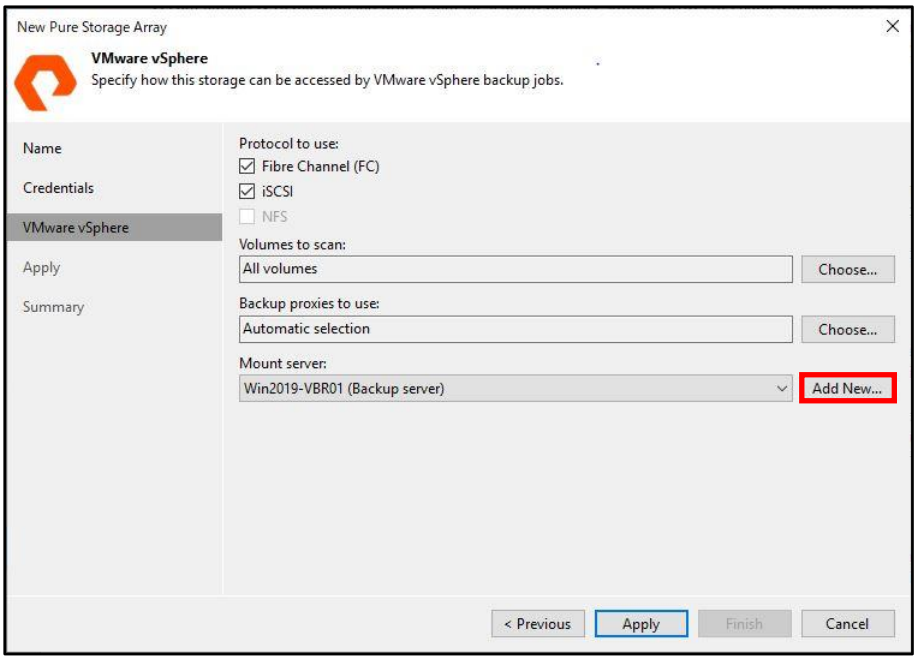
11. [Next >]をクリックします。



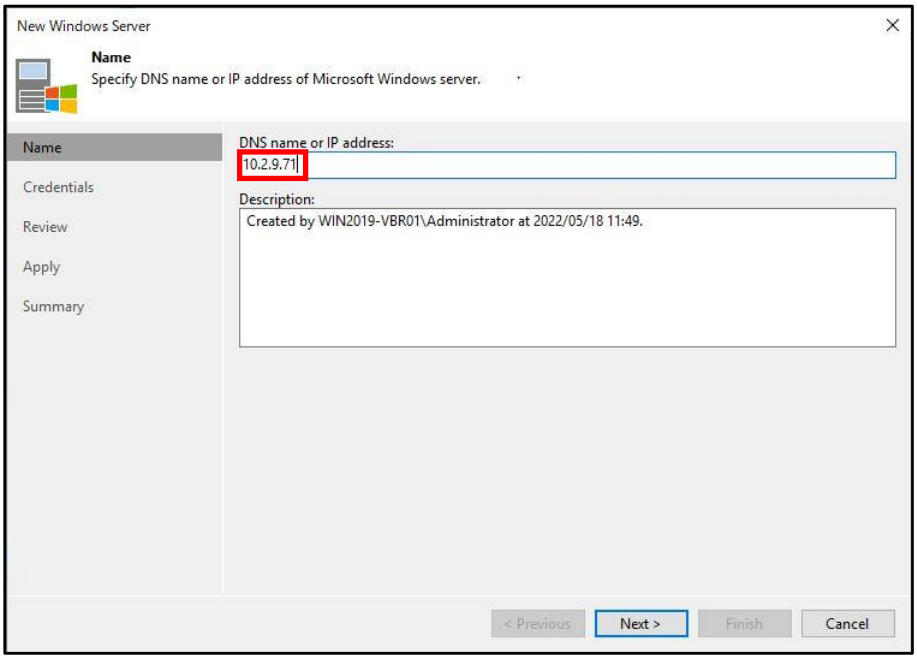
12. 環境に応じて FC・iSCSI にチェックします。



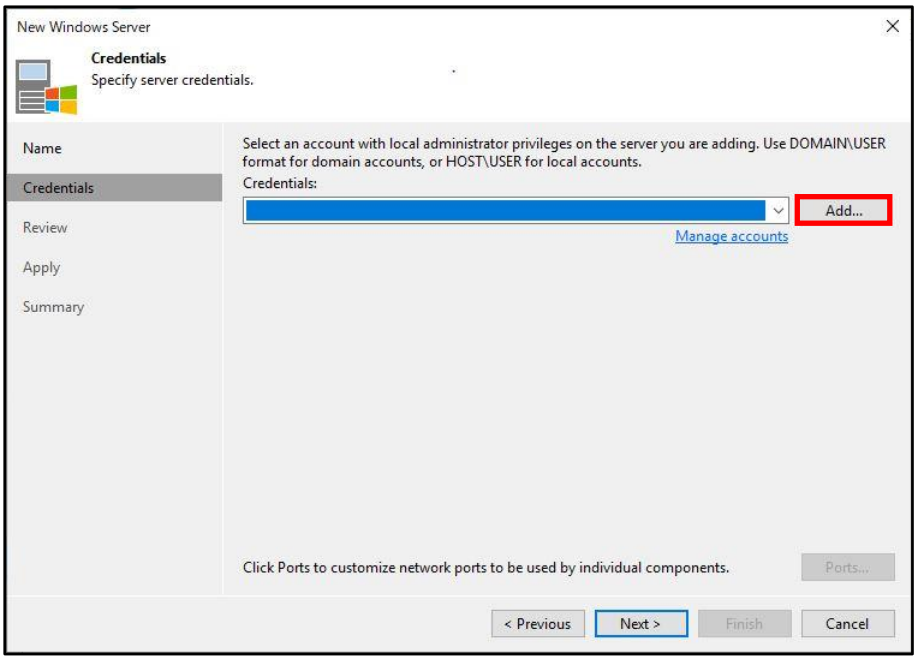
13. Mount server を追加しますので、[Add New...]をクリックします。



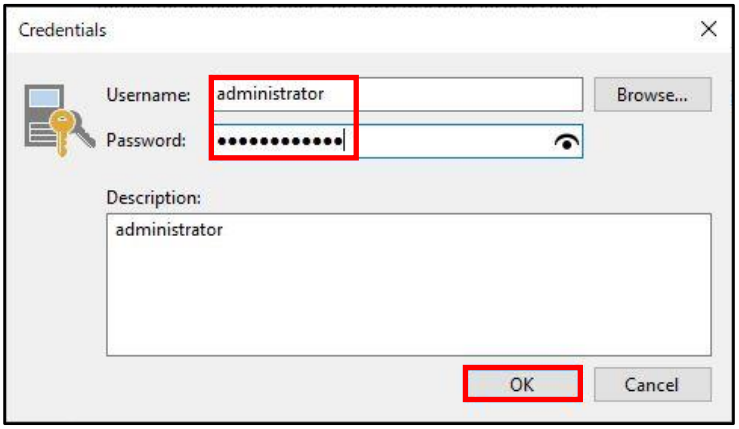
14. [DNS name or IP address:]に Mount server の FQDN または IP アドレスを入力します。



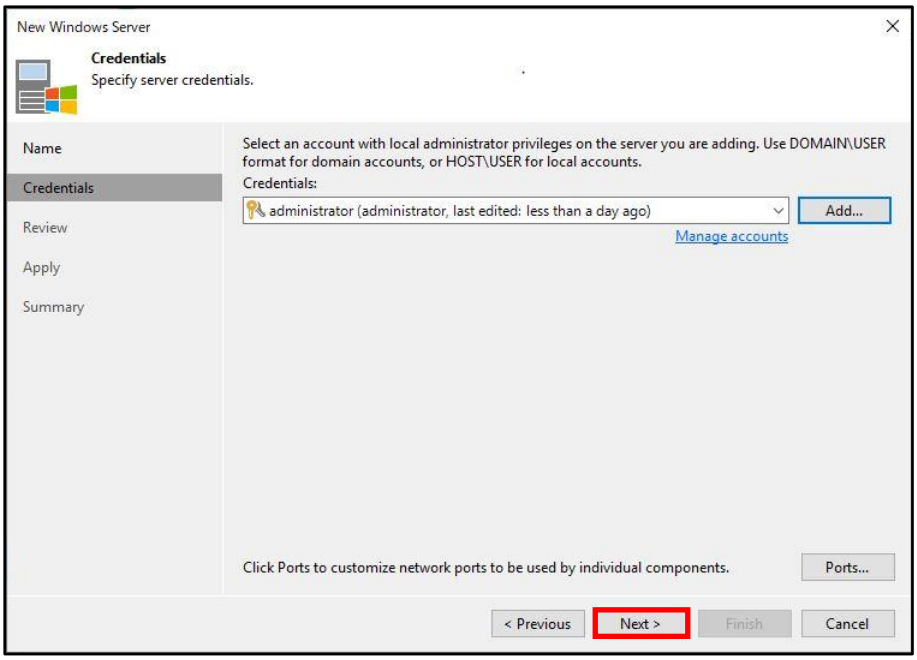
15. [Add...]をクリックします。



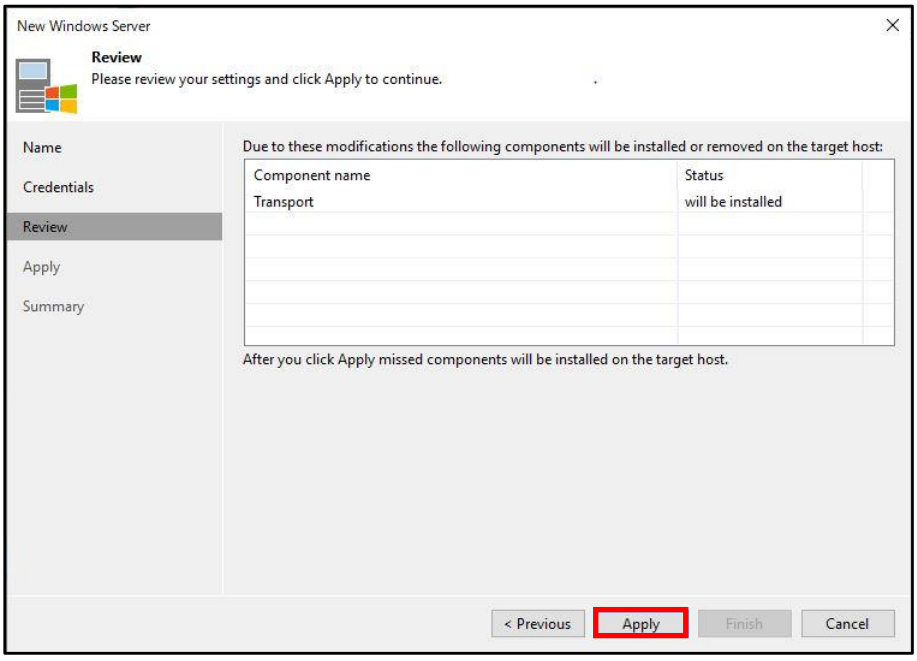
16. Mount server の Username と Password を入力して、[OK]をクリックします。
※本書では、[administrator]を使用します。



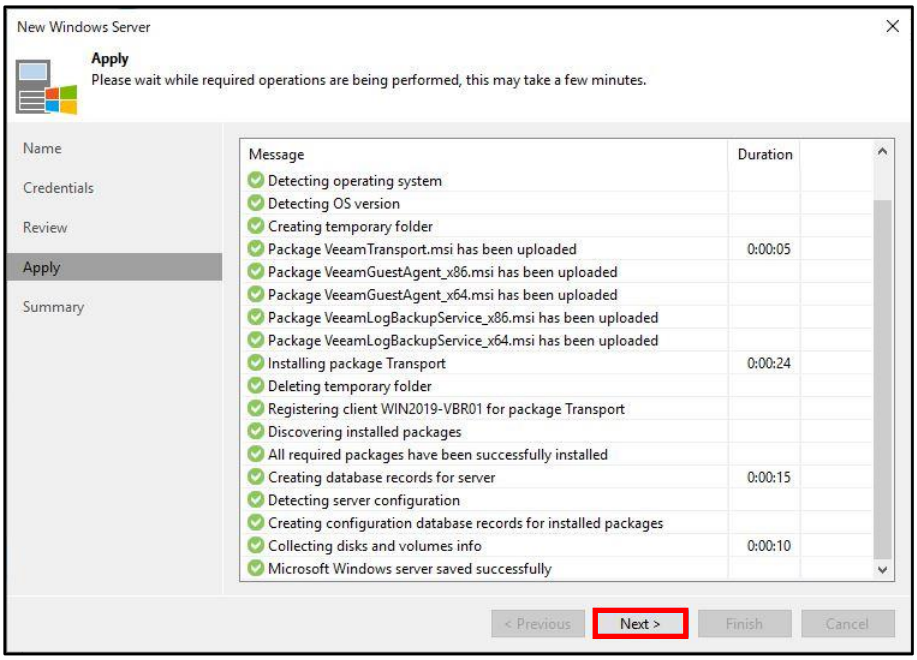
17. [Next >]をクリックします。



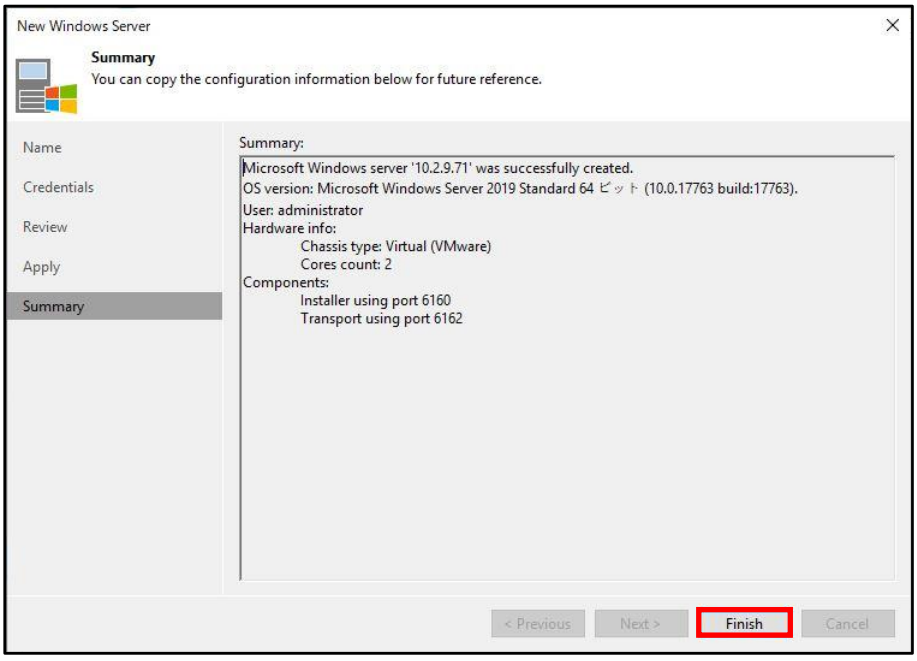
18. [Apply]をクリックします。



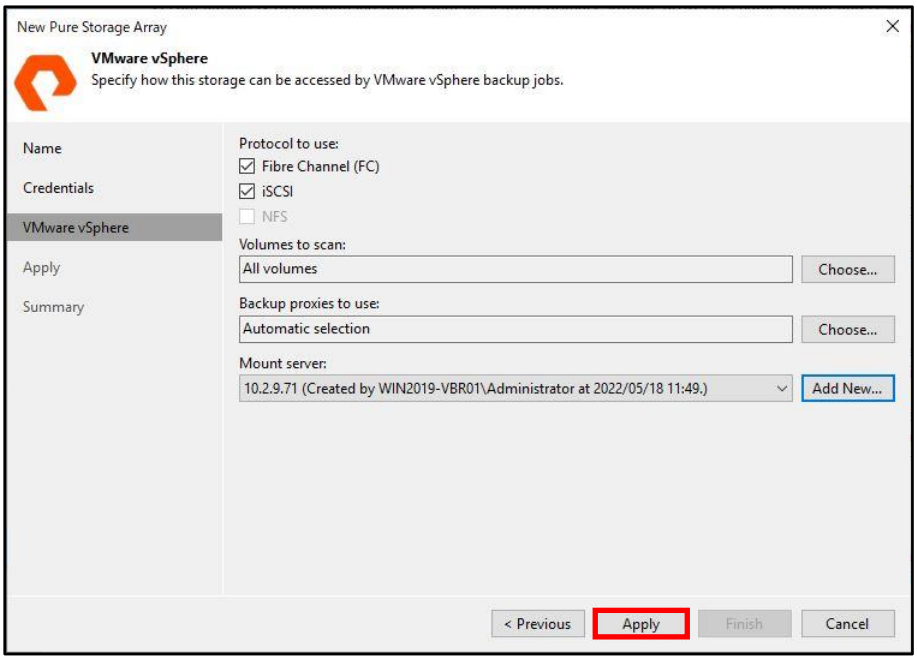
19. [Next >]をクリックします。



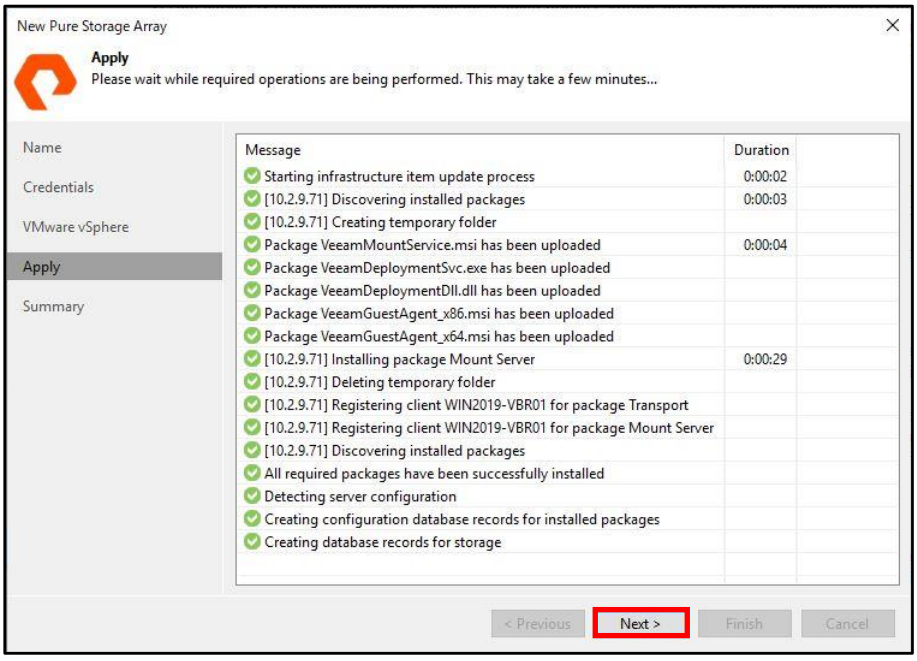
20. [Finish]をクリックします。



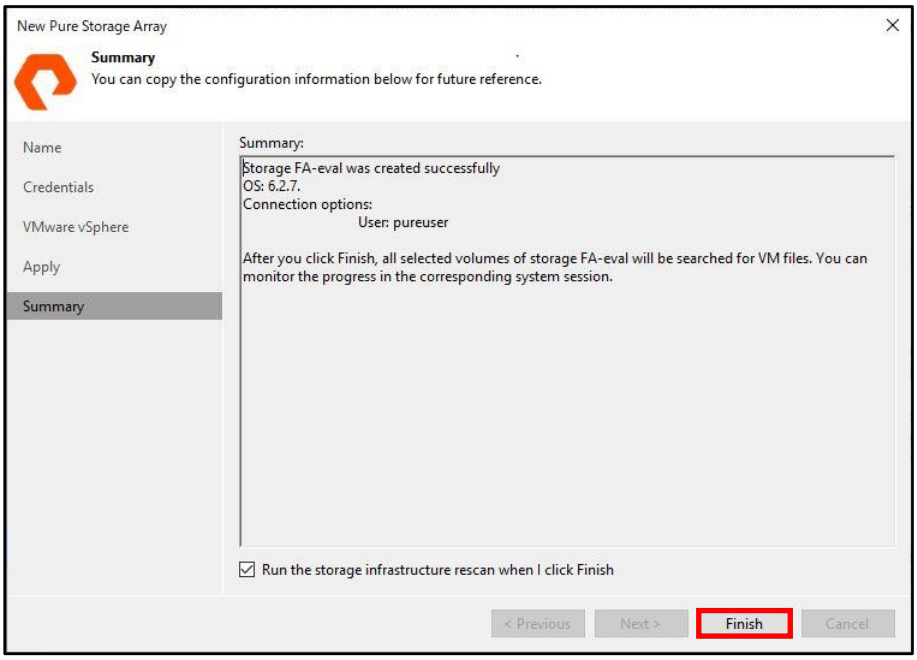
21. [Apply]をクリックします。



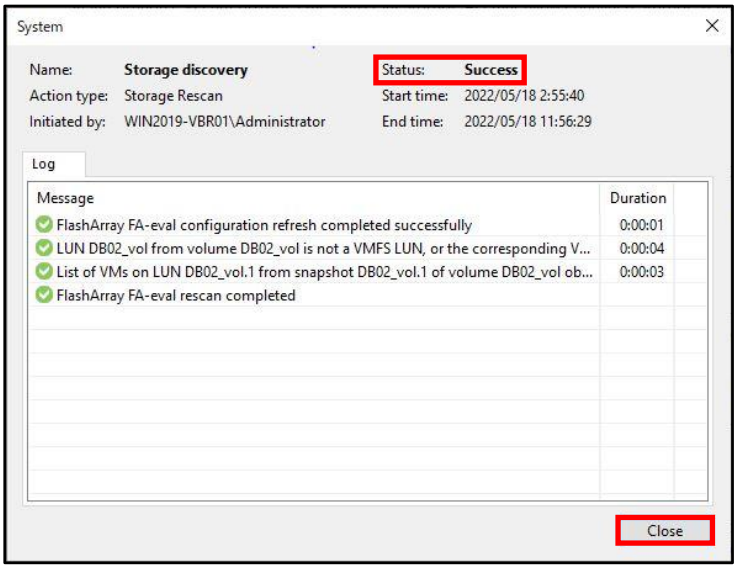
22. [Next >]をクリックします。



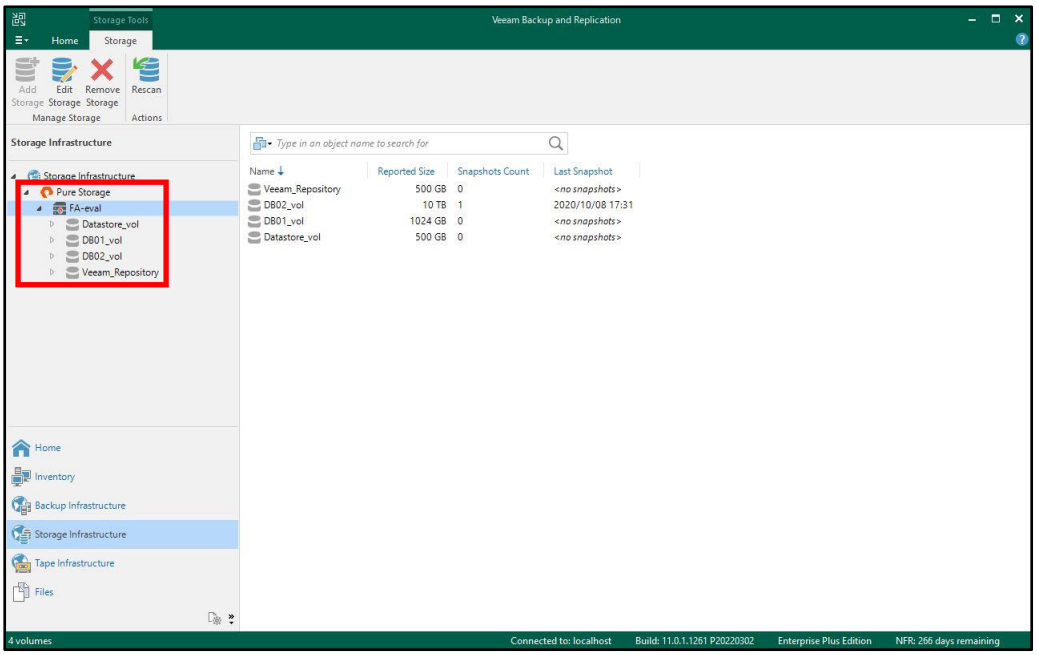
23. [Finish]をクリックします。



24. Status が[Success]で完了していることを確認して、[Close]をクリックします。



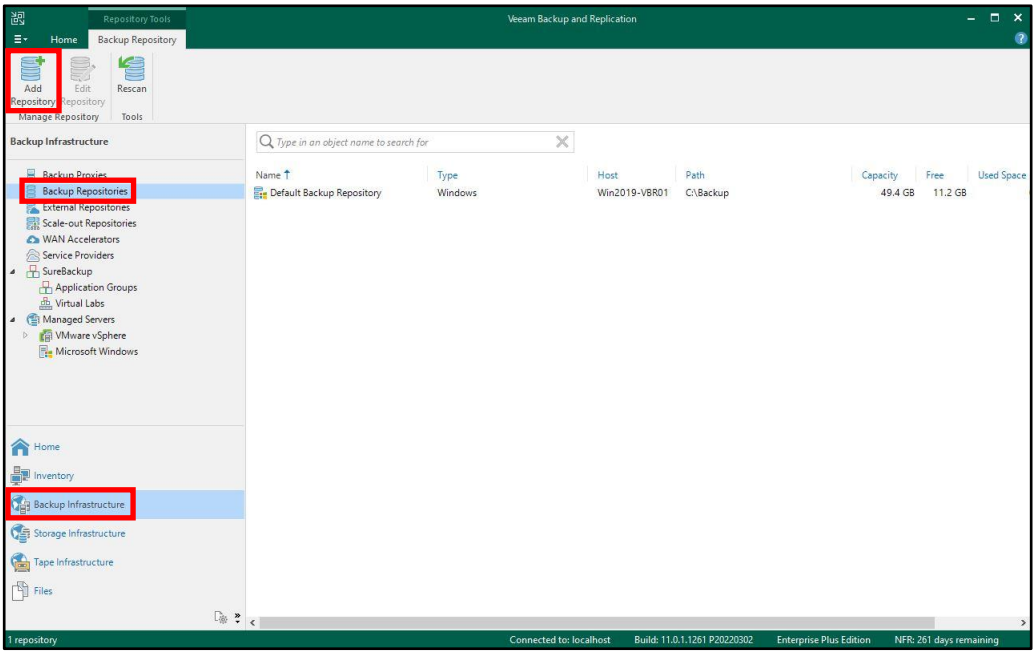
25. [Storage Infrastructure]-[Pure Storage]の[▶]をクリックして、ディレクトリが表示されることを確認します。



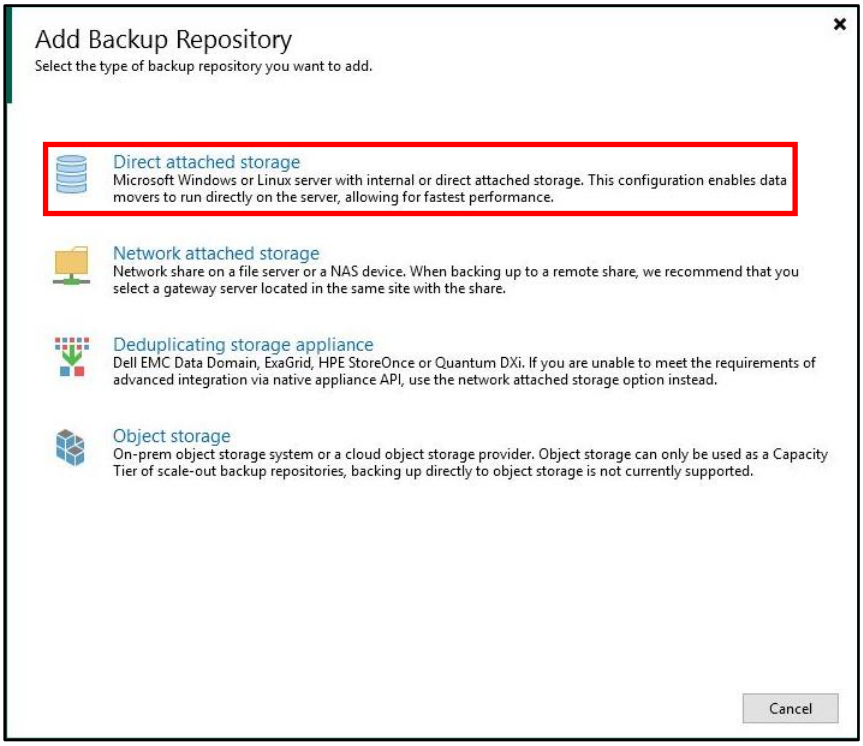
以上で Pure Storage の STORAGE INFRASTRUCTURE としての登録が完了となります。

6.1.3. 強化(書き換え不能)Linux リポジトリの登録手順

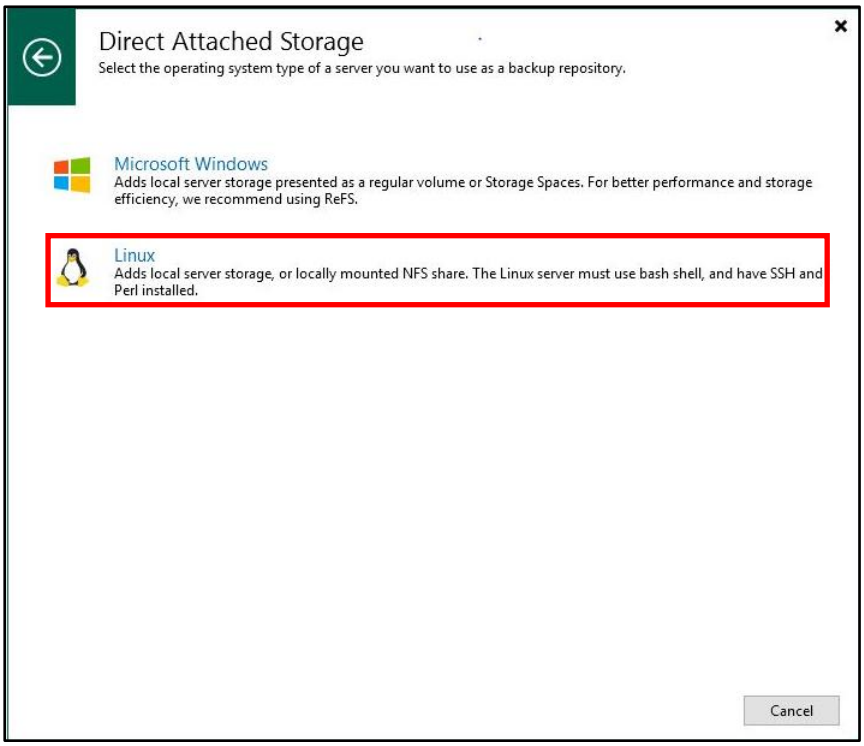
1. [Backup Infrastructure]-[Backup Repositories]-[Add Repository]をクリックします。



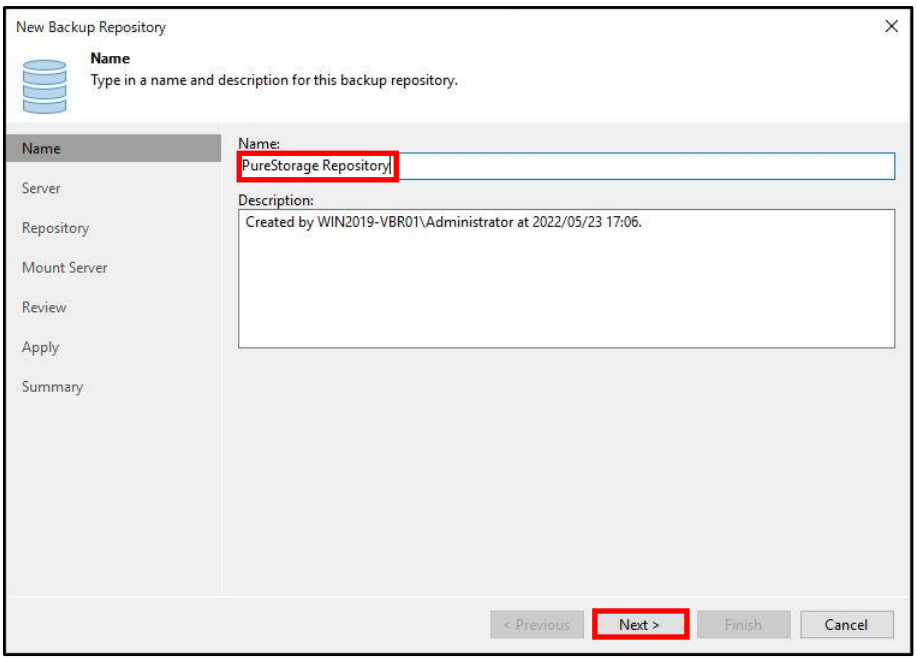
2. [Direct attached storage]をクリックします。



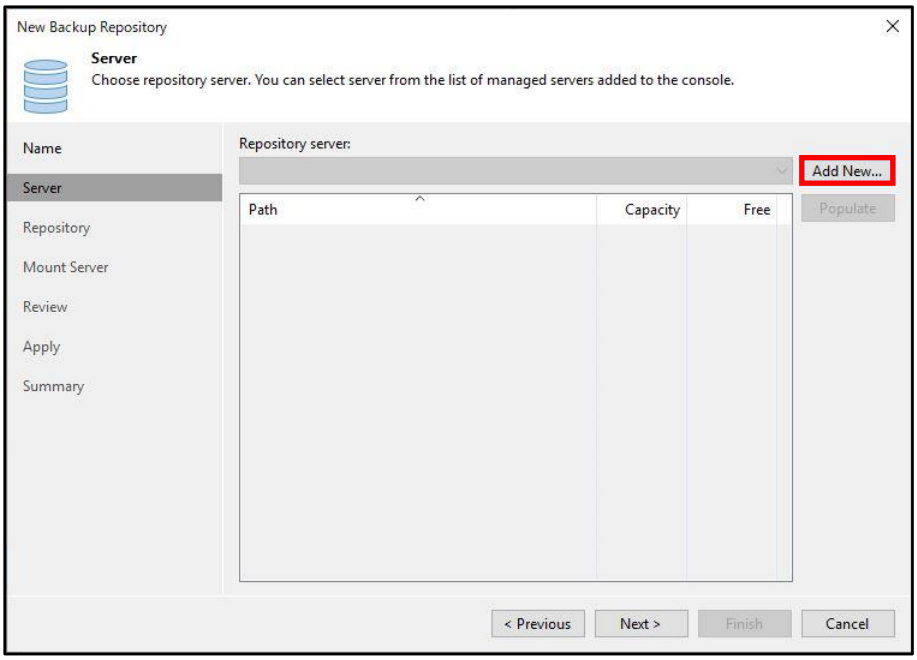
3. [Linux]をクリックします。



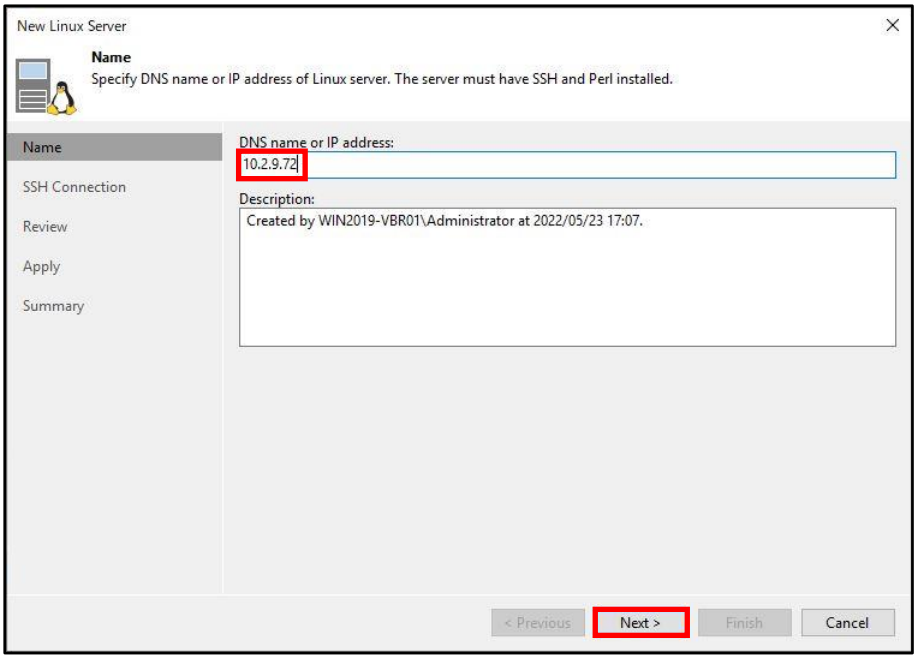
4. [Name]に任意の Repository 名を入力して、[Next >]をクリックします。



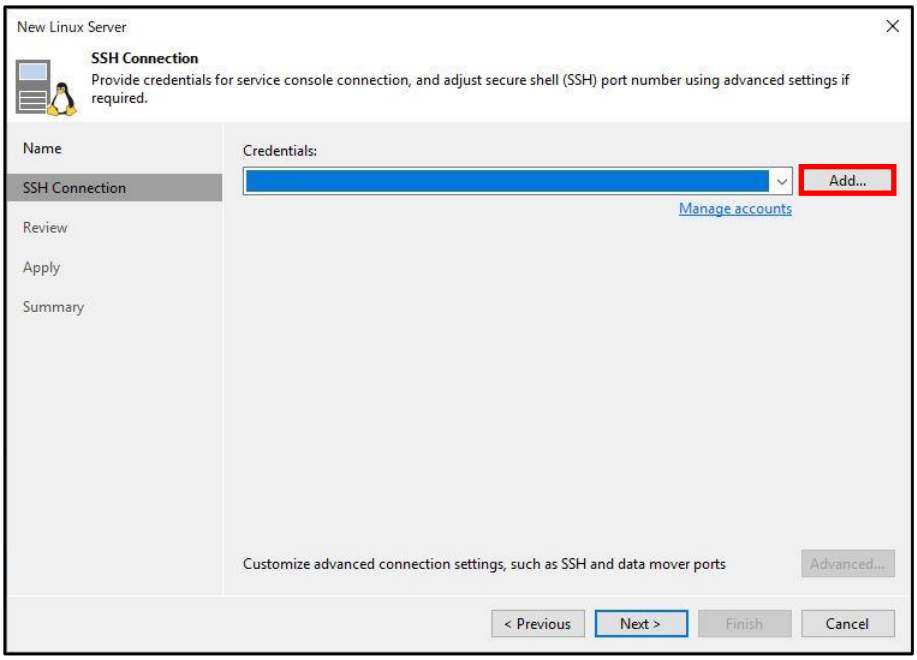
5. Linux リポジトリを追加しますので、[Add New...]をクリックします。



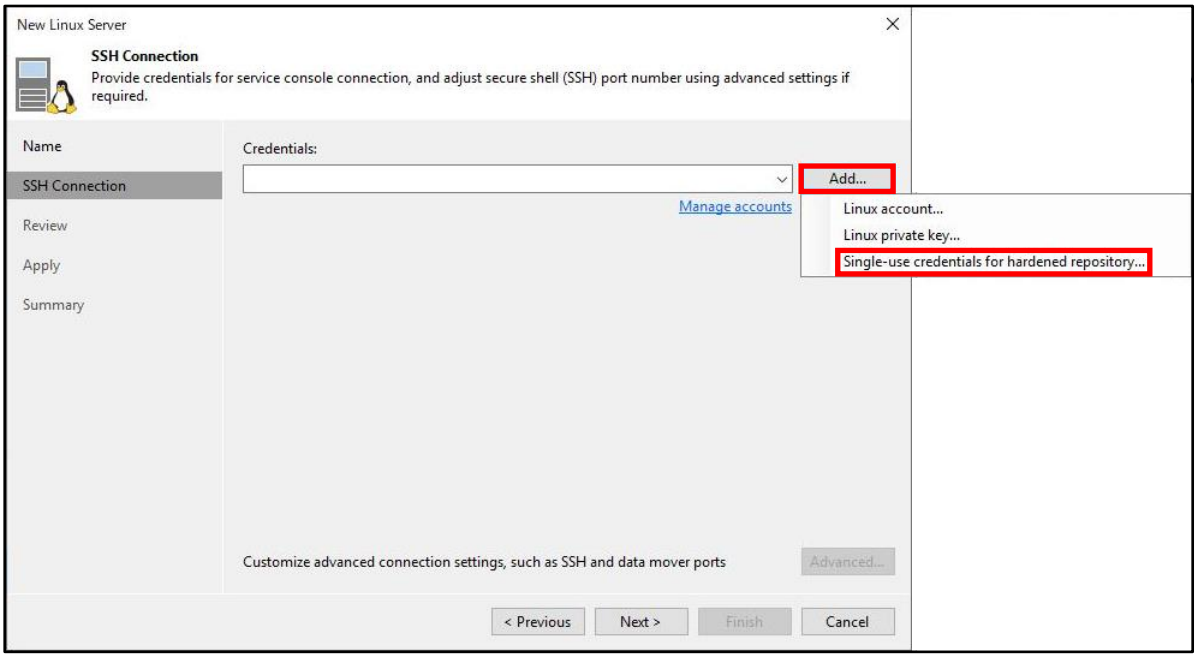
6. [DNS name or IP address:]に Linux Repository の FQDN または IP アドレスを入力します。



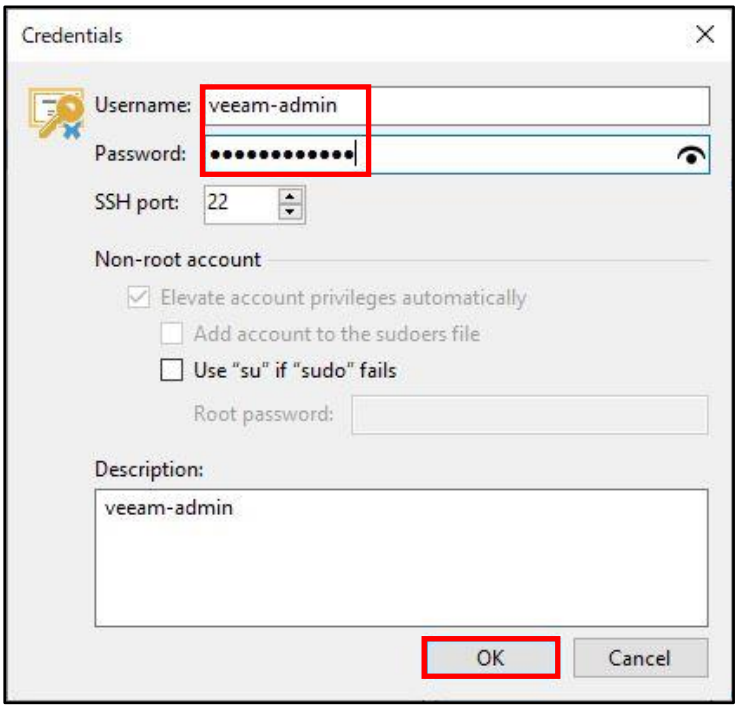
7. [Add...]をクリックします。



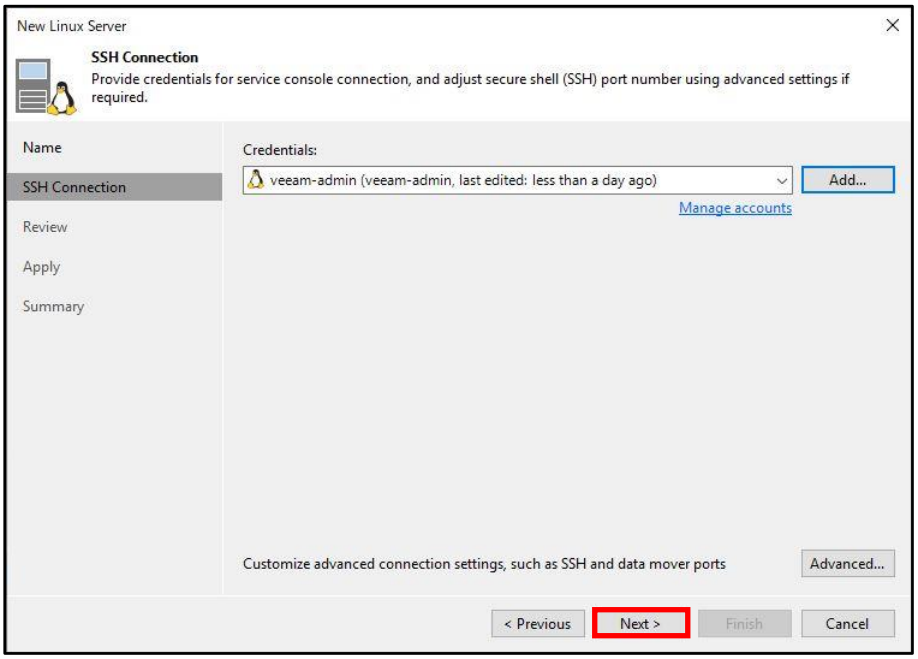
8. [Add...]-[Single-use credentials for hardened repository...]をクリックします。
※「Single-use credentials for hardened repository」を選択した場合、Veeam Backup & Replication にログイン情報は保存されません。またログイン情報は、Veeam データムーバーサービスをホストに導入する際にのみ使用されますのでセキュリティを向上できます。



9. Linux リポジトリの Username と Password を入力して、[OK]をクリックします。
※本書では、[veeam-admin]を使用します。

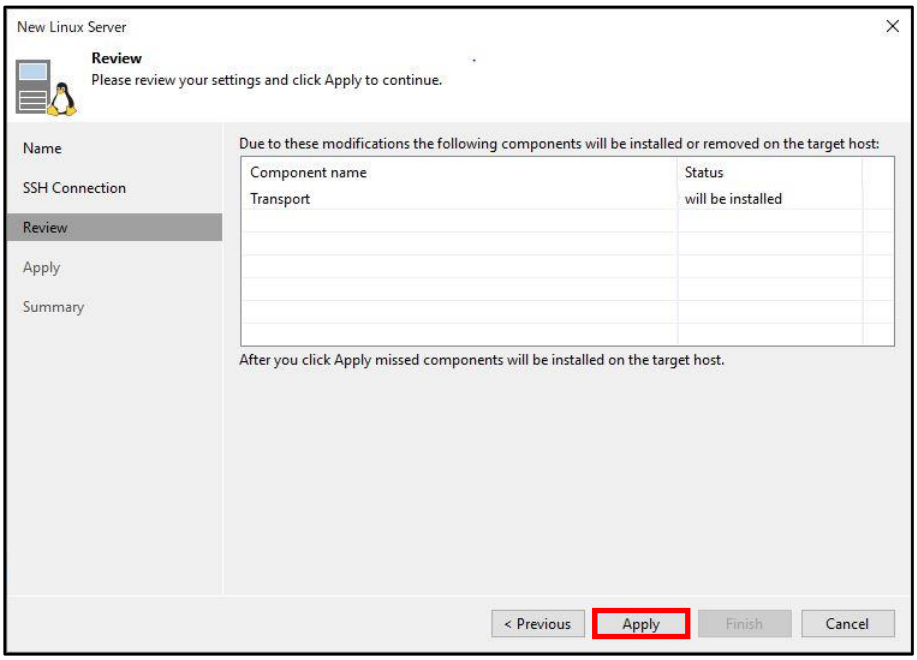


10. [Next >]をクリックします。

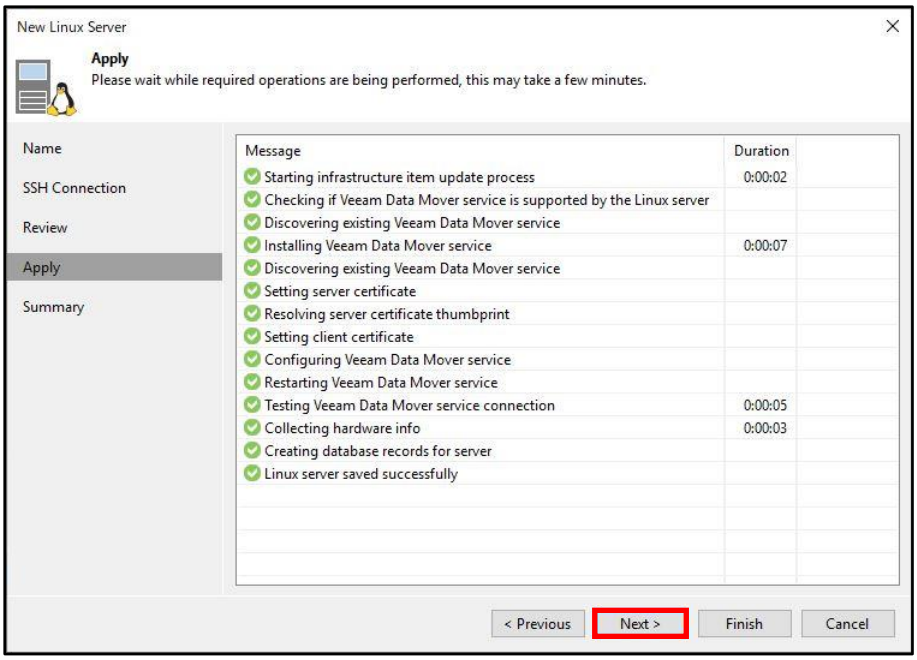


11. SSH key に関する警告が出ますが、そのまま[Yes]をクリックします。

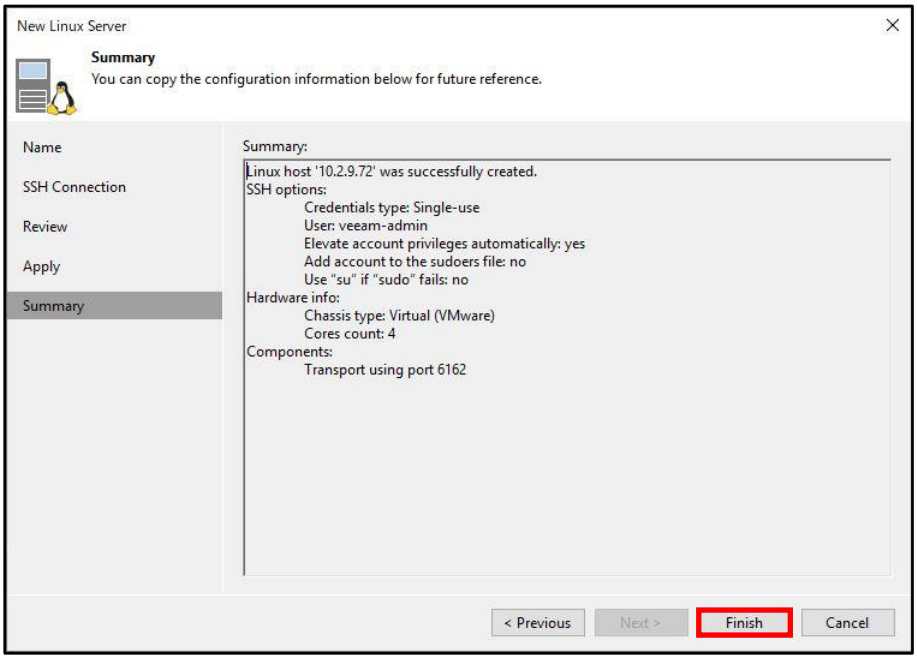
12. [Apply]をクリックします。



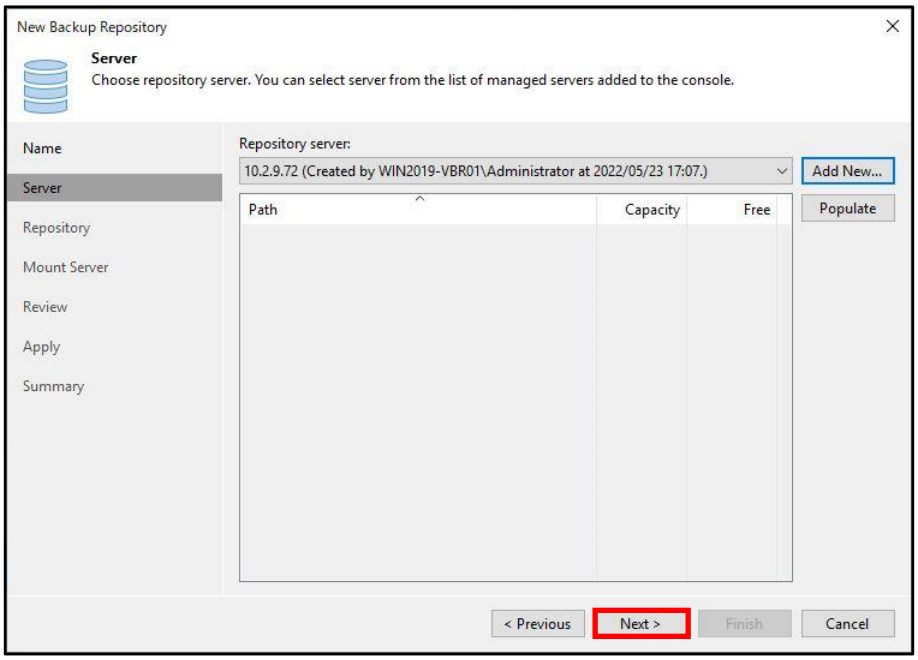
13. [Next >]をクリックします。



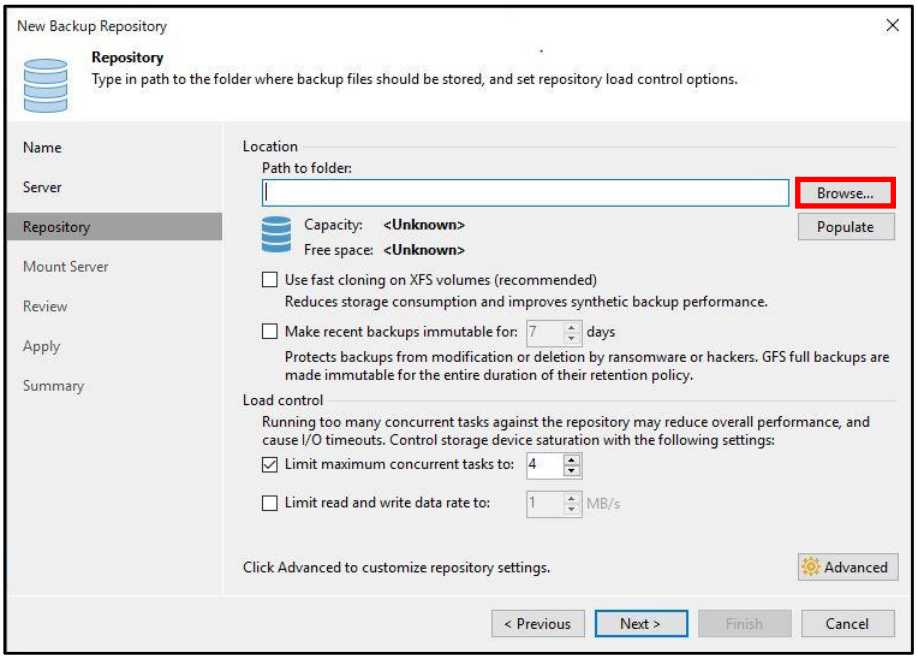
14. [Finish]をクリックします。



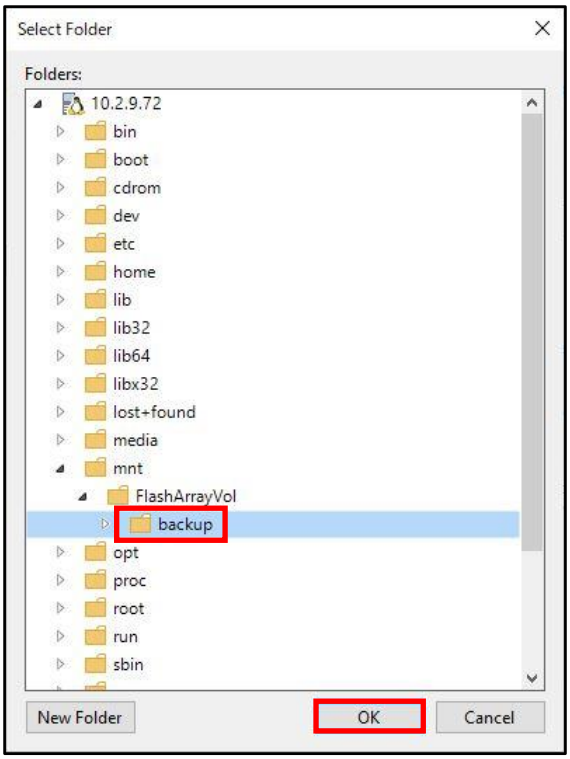
15. [Next >]をクリックします。



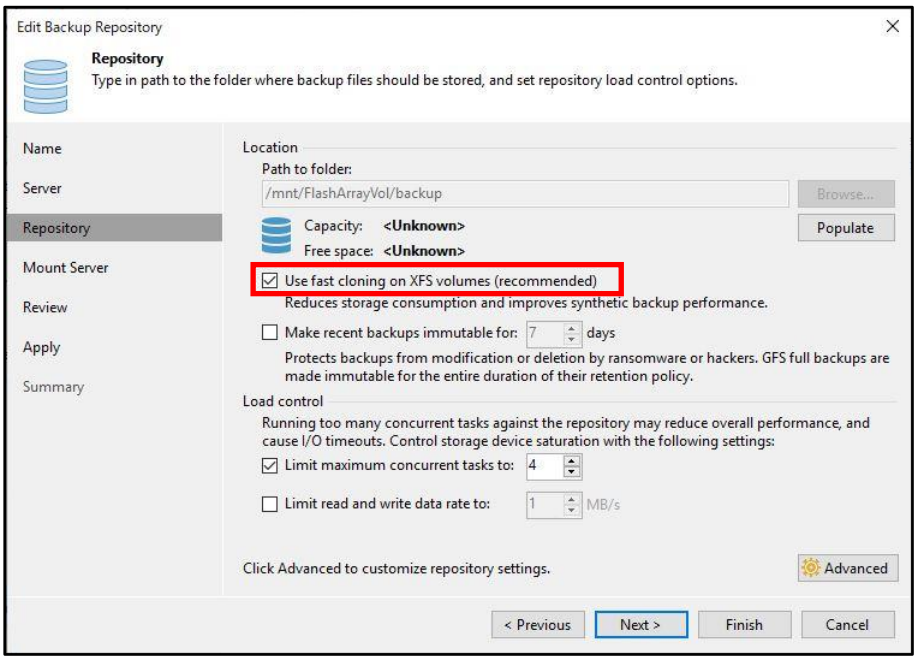
16. [Browse...]をクリックします。



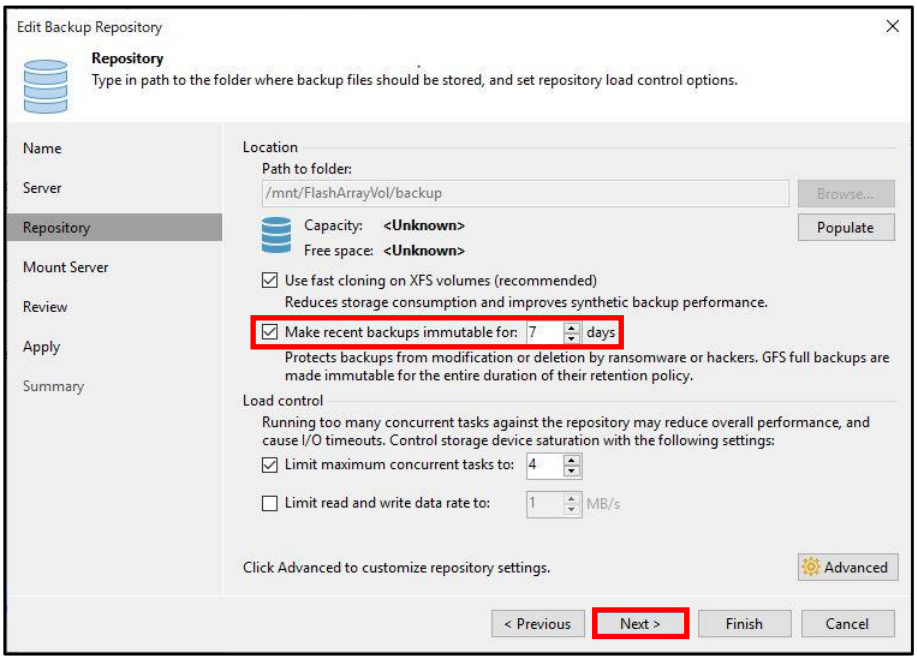
17. 事前に作成した[backup]フォルダを選択して、[OK]をクリックします。



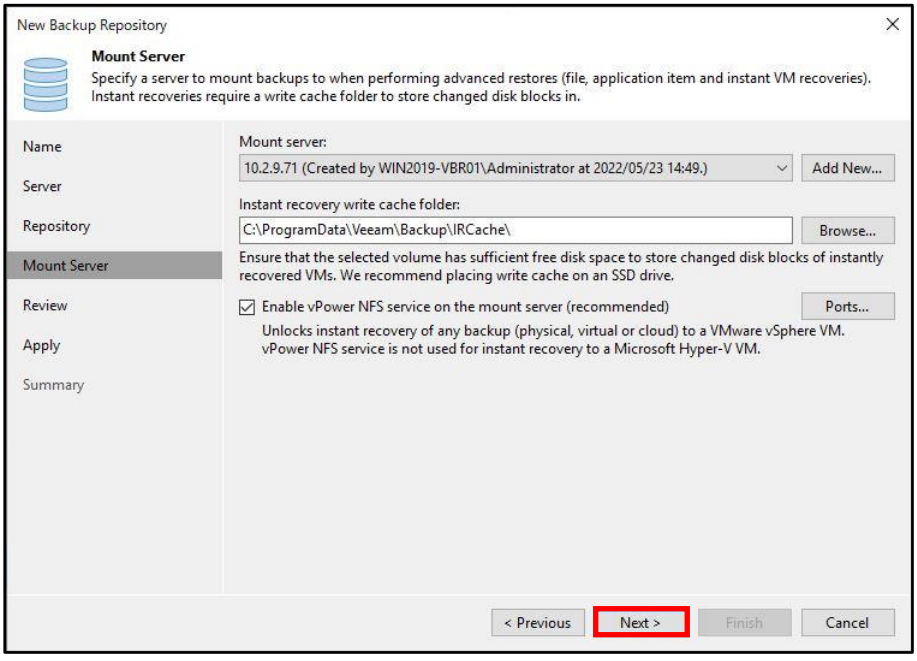
18. [Use fast cloning on XFS volumes(recommended)]にチェックします。
※XFS の適用は Fast Clone による容量削減効果が見込めるため、推奨設定となります。
ファイルシステム構成時の詳細オプションは以下を参照ください。
https://helpcenter.veeam.com/docs/backup/vsphere/backup_repository_block_cloning.html?ver=110#fast-clone-for-linux-repositories



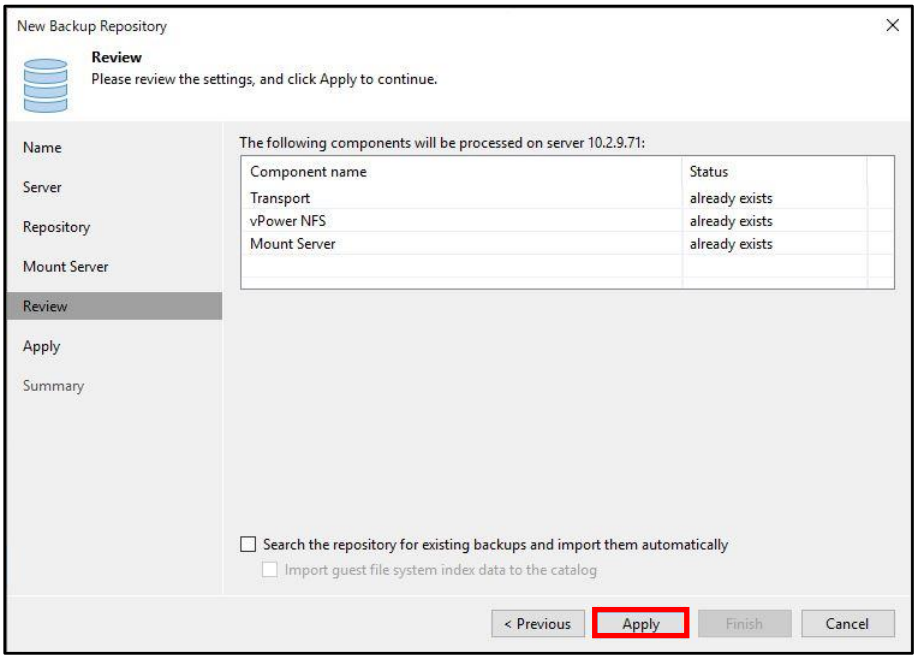
19. [Make recent backups immutable:]にチェックして、[Next >]をクリックします。
※本書では、デフォルトの[7days]を使用します。



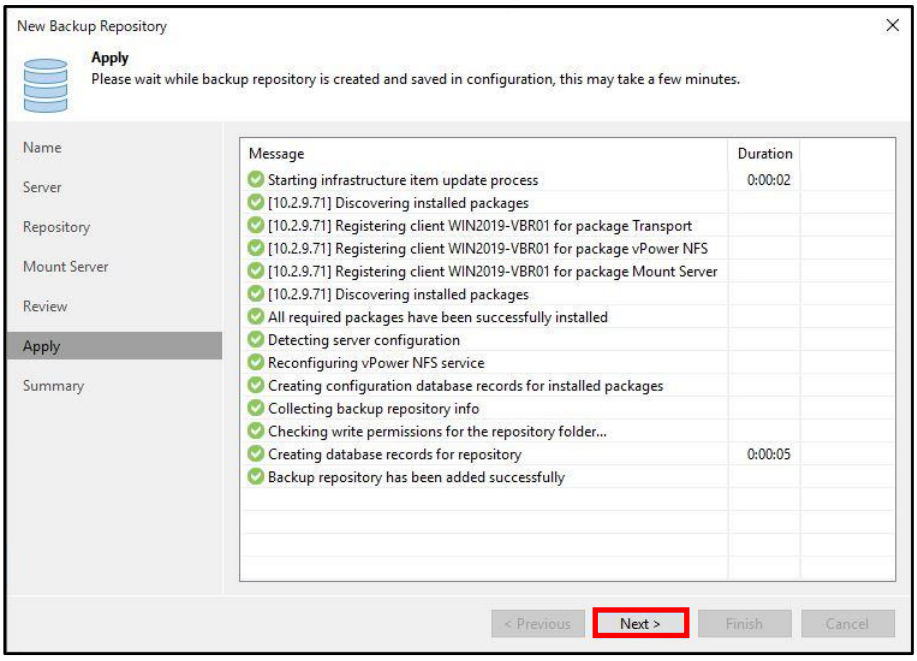
20. [Next >]をクリックします。



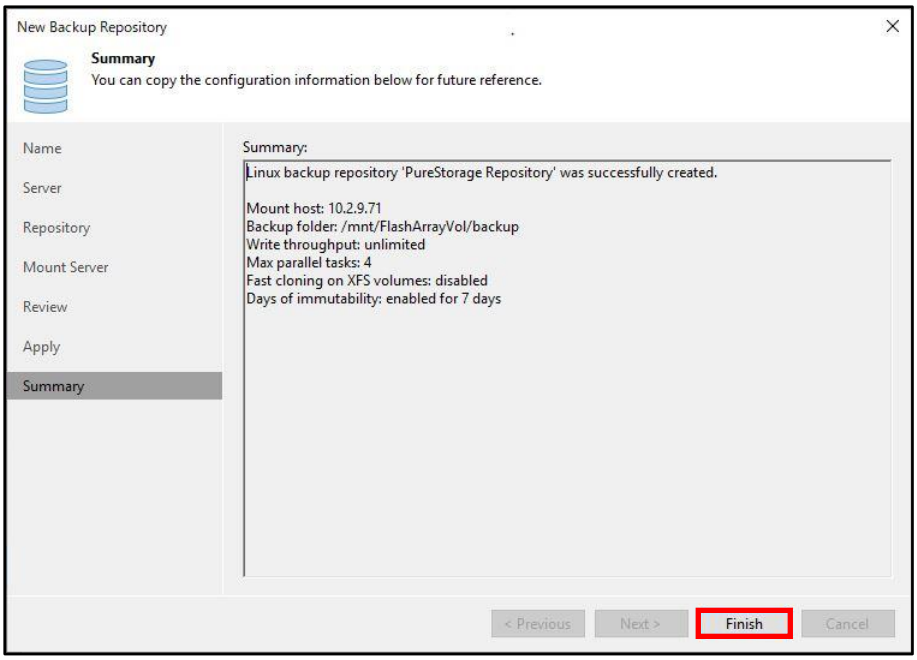
21. [Apply]をクリックします。



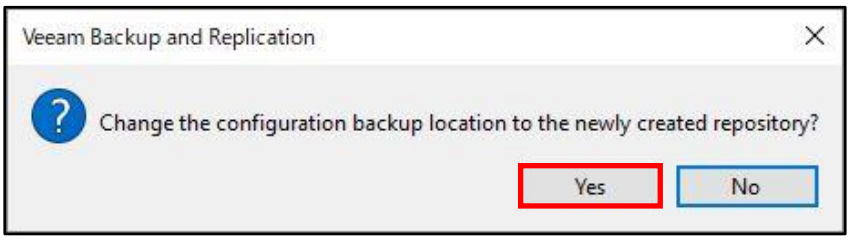
22. [Next >]をクリックします。



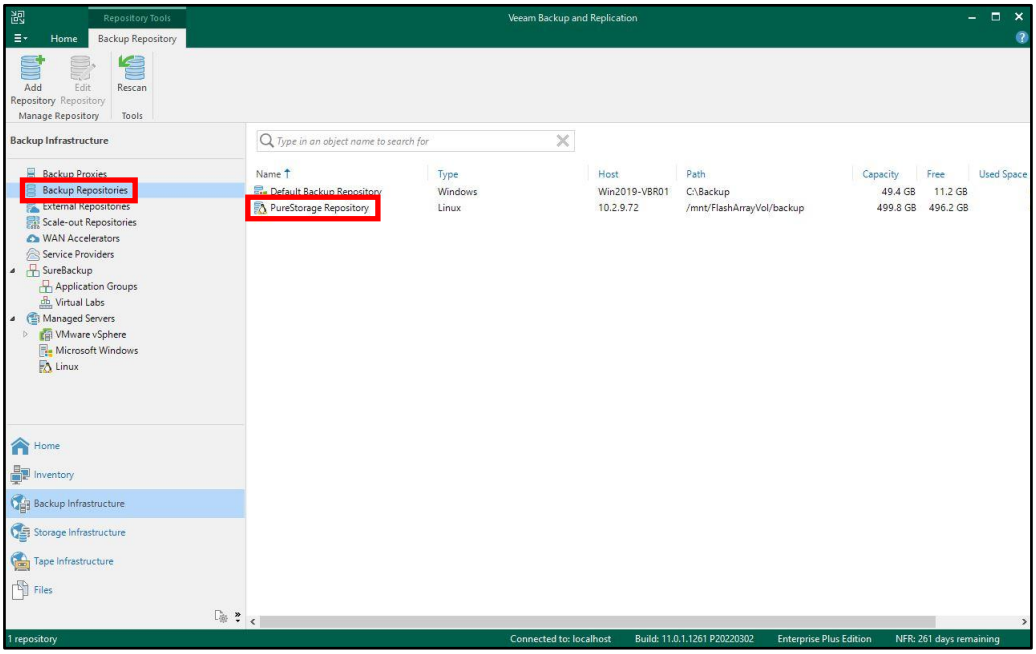
23. [Finish]をクリックします。



24. configuration backup の保存先を変更する場合は、「Yes」をクリックします。
本手順では、そのまま[Yes]をクリックします。



25. Linux リポジトリが追加されたことを確認します。



26. Linux リポジトリサーバーにログインして SSH を無効化します。

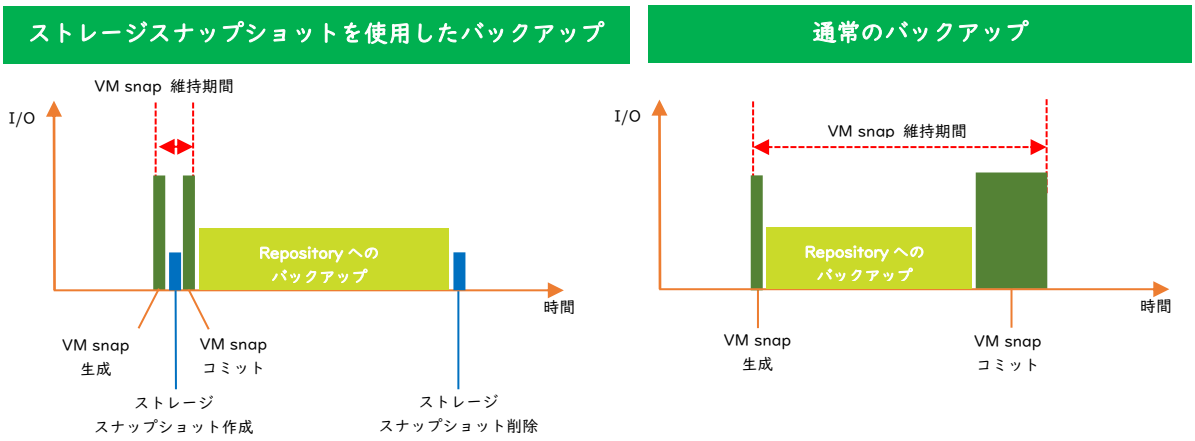
```
veeam-admin@Linux-Repository01:~$
veeam-admin@Linux-Repository01:~$
veeam-admin@Linux-Repository01:~$ sudo systemctl stop ssh
[sudo] veeam-admin のパスワード:
veeam-admin@Linux-Repository01:~$
veeam-admin@Linux-Repository01:~$
```

以上で Pure Storage の Repository としての登録が完了となります。

6.2. バックアップ

Veeam はストレージスナップショットと連携することにより、仮想マシンのスナップショット維持時間を短縮し、下記の課題を回避するとともにバックアップを高速化します。

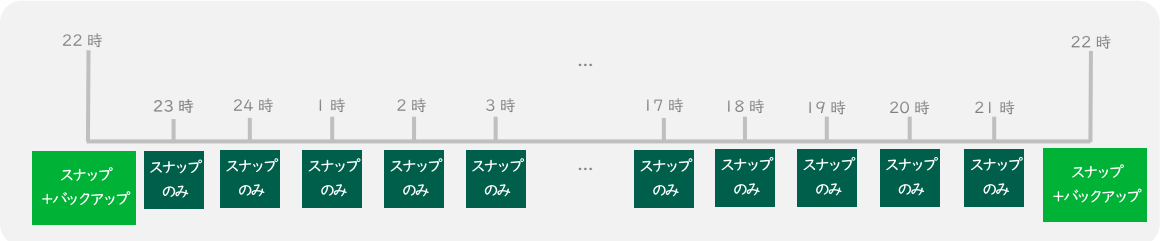
<連携機能①ストレージスナップショットを使用したバックアップ>
vSphere 環境の仮想マシンのバックアップでは仮想マシンのスナップショットを利用します。仮想マシンのスナップショット作成時に構成される、読み取り専用の仮想ディスクからバックアップデータをコピーします。バックアップデータを取得するには効果的ですが、差分ディスクへの更新量が多い場合、コミットに時間がかかり VM Stun が起きる原因となるといった課題もあります。Veeam のストレージスナップショット連携により仮想マシンスナップショットをストレージにオフロードすることにより、コミット時間に関する課題を解消することが可能です。



<連携機能②スナップショットオーケストレーション>
バックアップ時の本番環境への影響を最小限に抑えて RPO をさらに改善するために、Veeam はスナップショットオーケストレーションというストレージスナップショット専用ジョブを活用することができます。

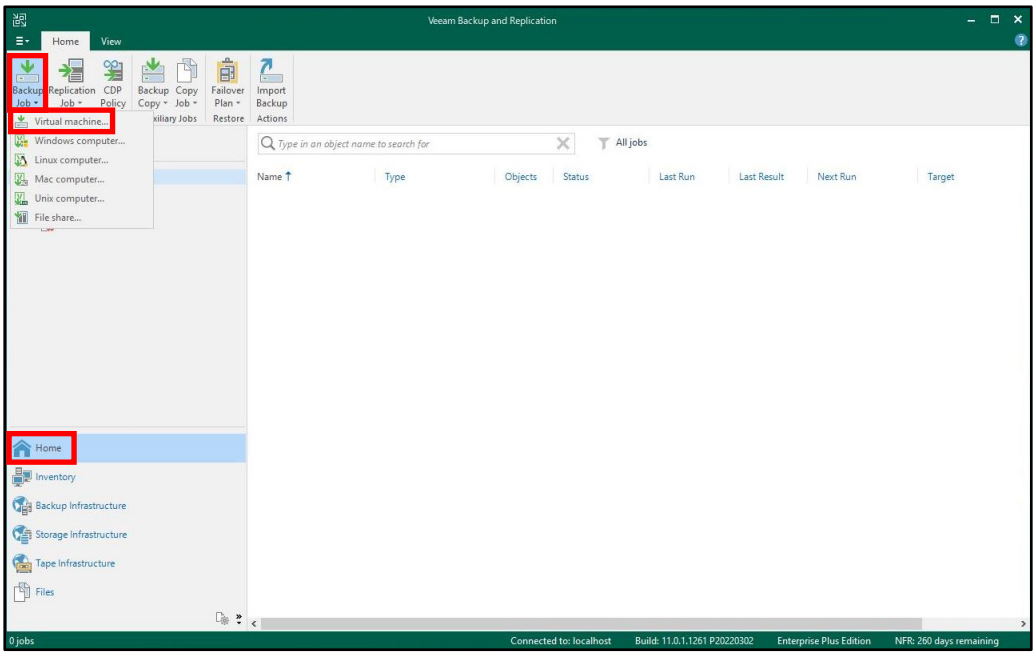
本書では、下記のスケジュールでバックアップを取得する手順を説明します。

- 毎日 22 時にストレージスナップショットを使用したバックアップジョブの実行
- 毎日 1 時間ごとにスナップショットオーケストレーションを使用したストレージスナップショット専用ジョブの実行

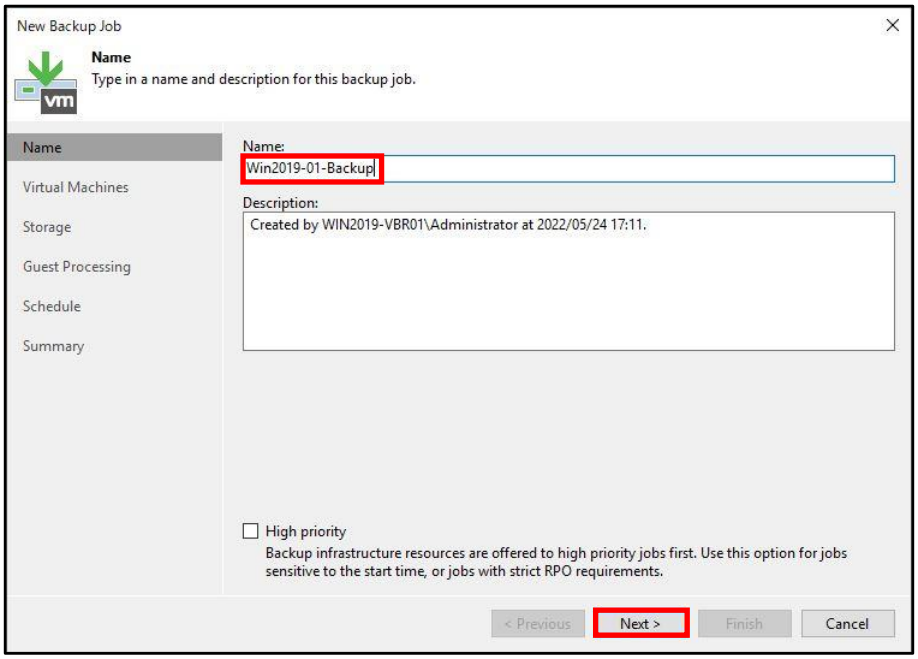


6.2.1. ストレージスナップショットを使用したバックアップ

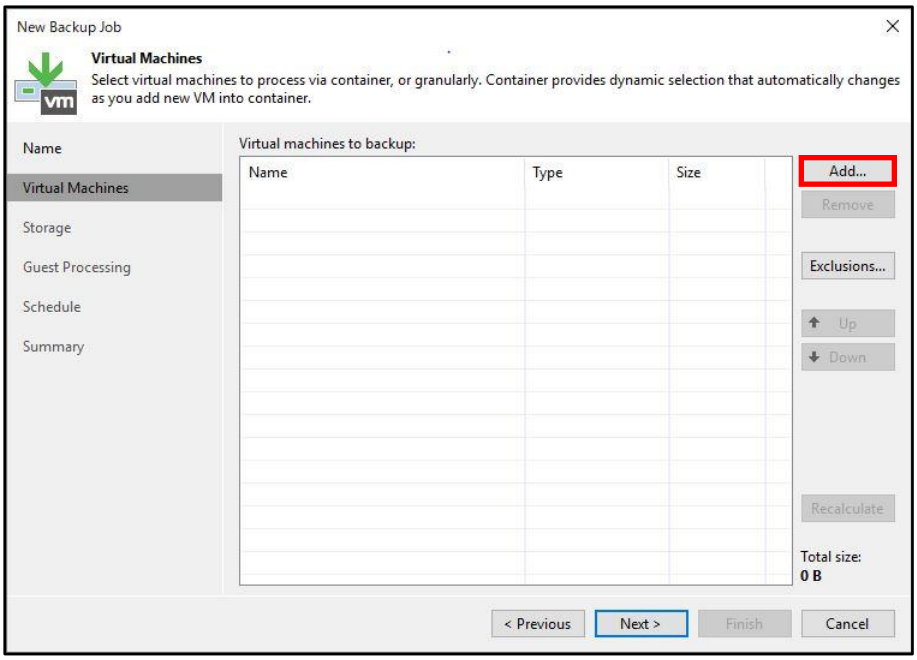
1. Veeam Backup & Replication Console の[HOME]-[Backup Job]-[Virtual machine...]をクリックします。



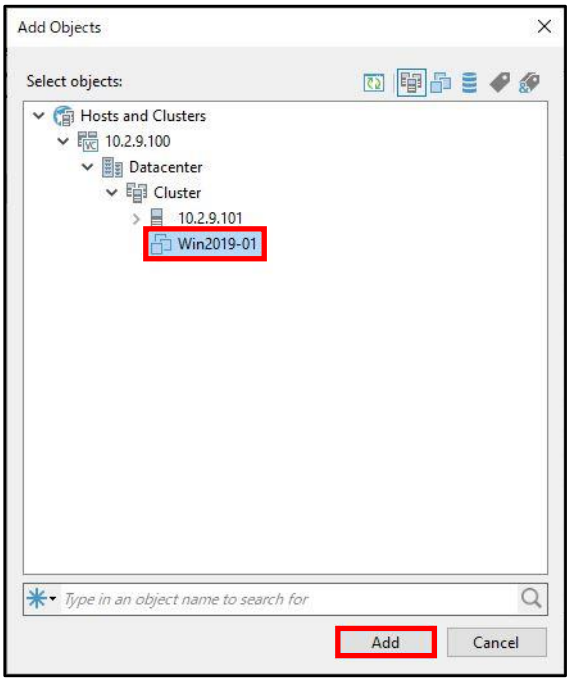
2. 任意のバックアップジョブ名を入力して、[Next >]をクリックします。



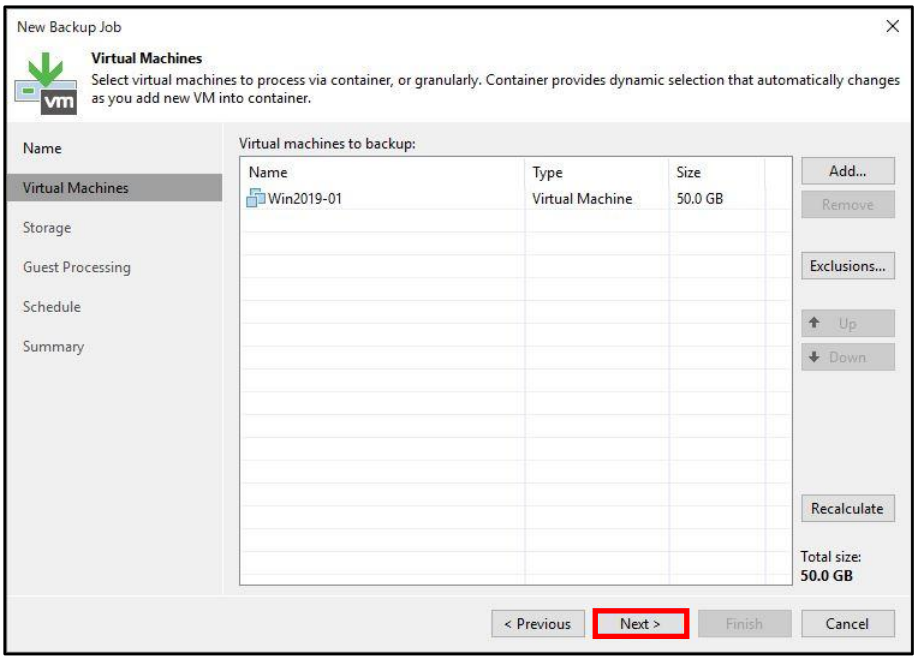
3. [Add...]をクリックします。



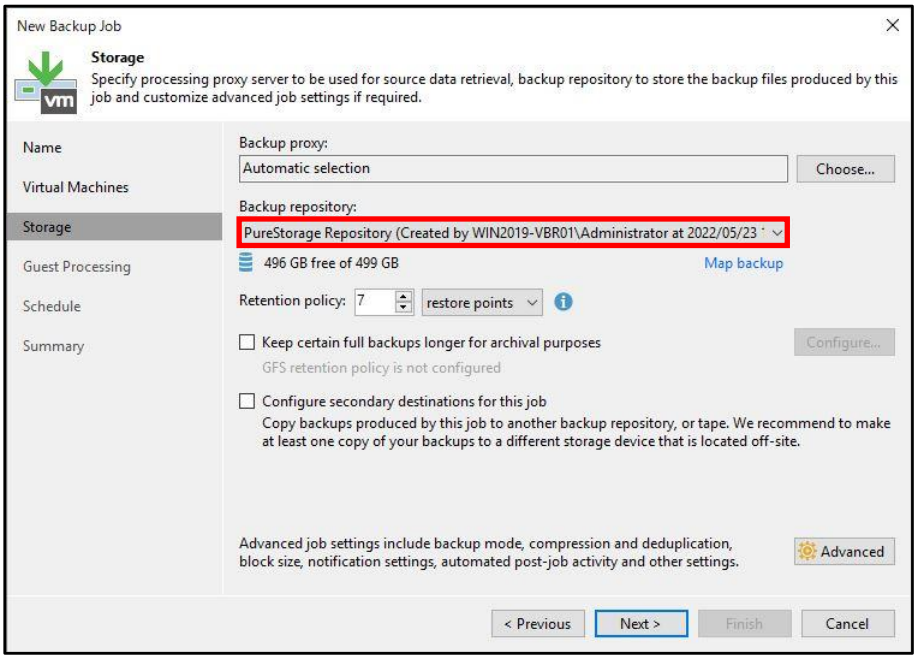
4. バックアップする仮想マシンを選択して、[Add]をクリックします。



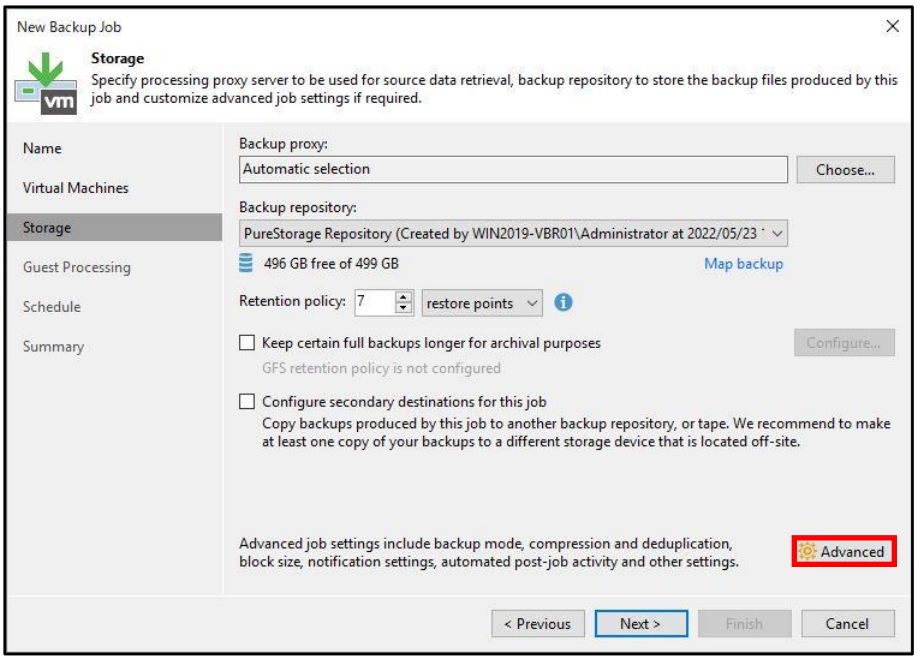
5. [Next >]をクリックします。



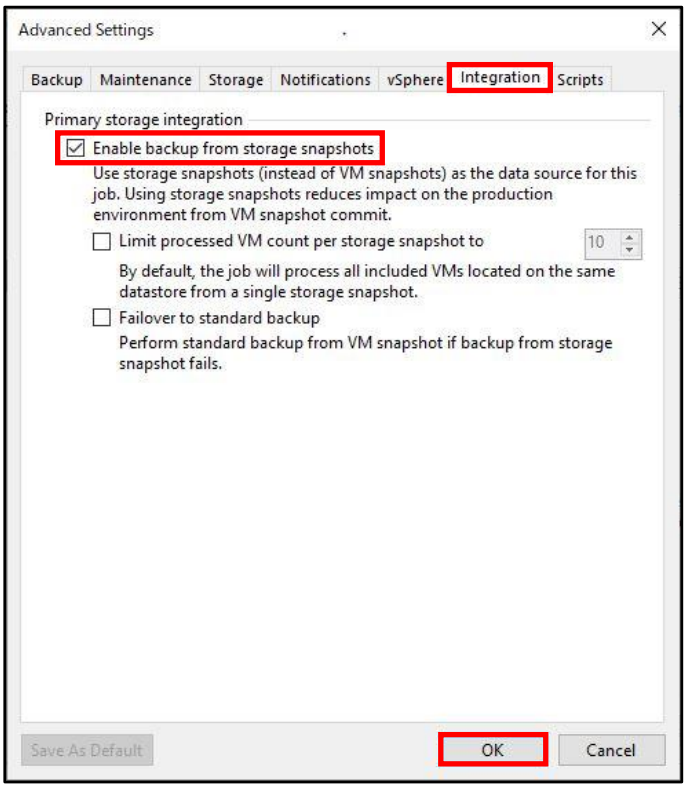
6. Backup repository を選択します。



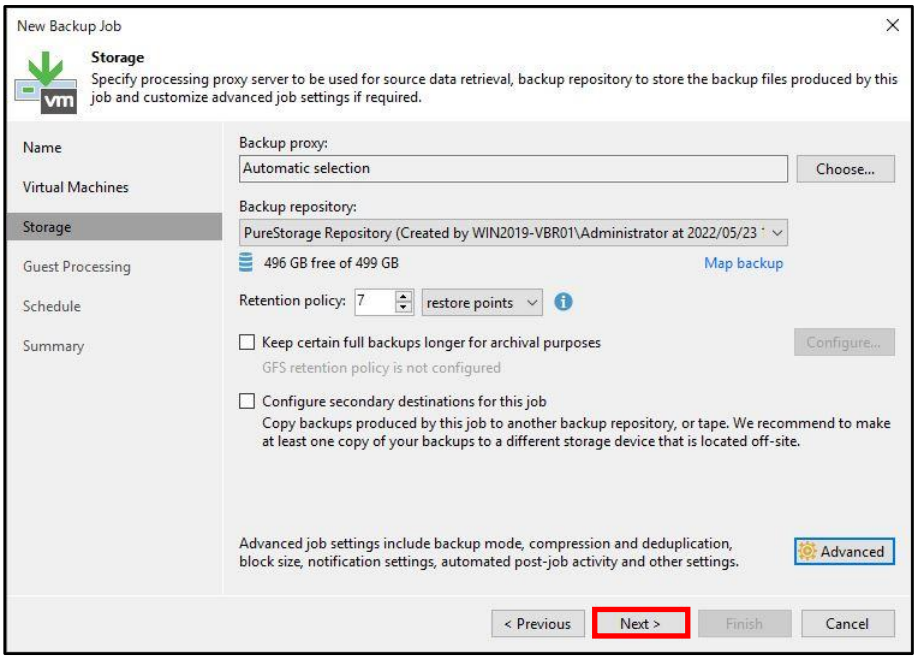
7. [Advanced]をクリックします。



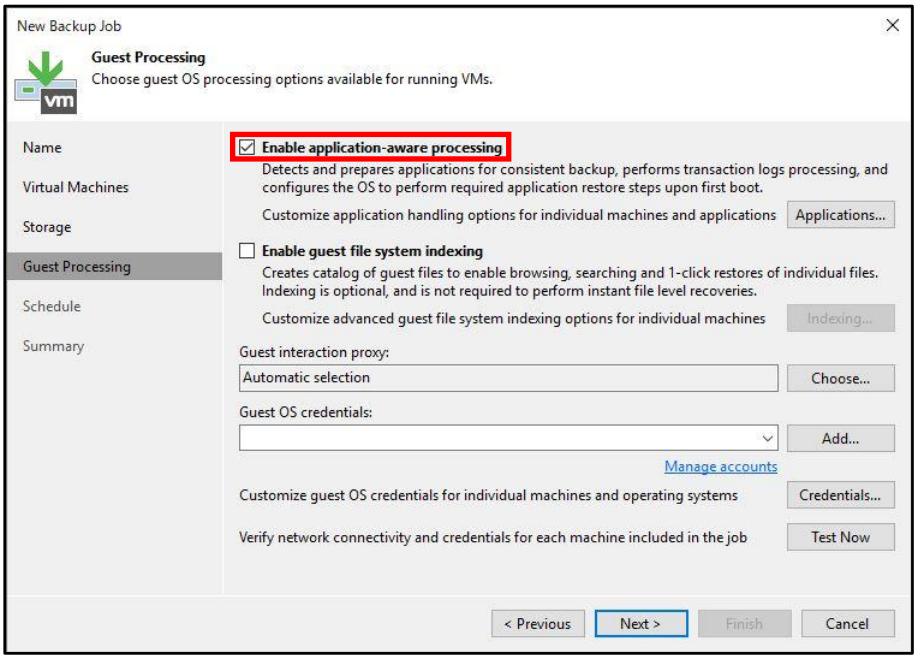
8. [Integration]タブ-[Enable backup from storage snapshots]がチェックされていることを確認して、そのまま[OK]をクリックします。 ※ストレージスナップショットを使用したバックアップを使用しない場合は、このチェックを外します。



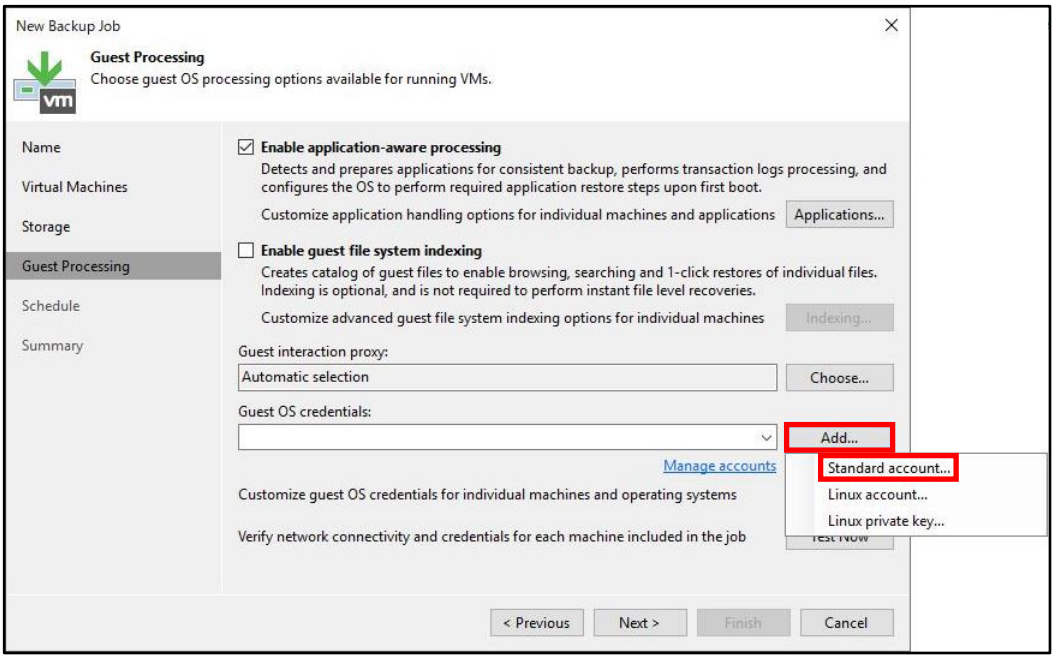
9. [Next >]をクリックします。



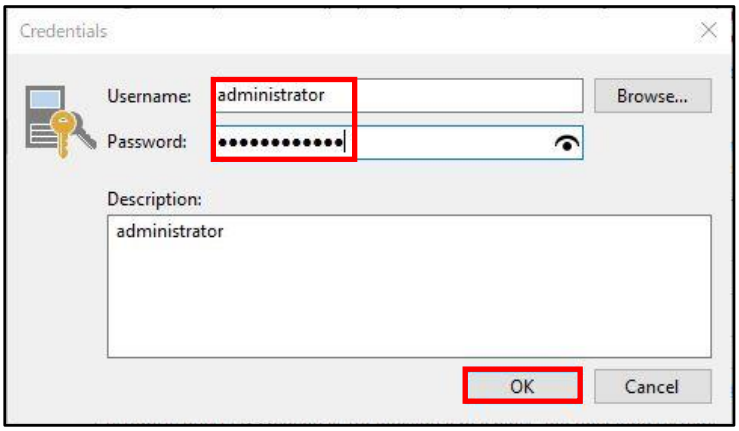
10. [Enable application-aware processing]にチェックを入れます。



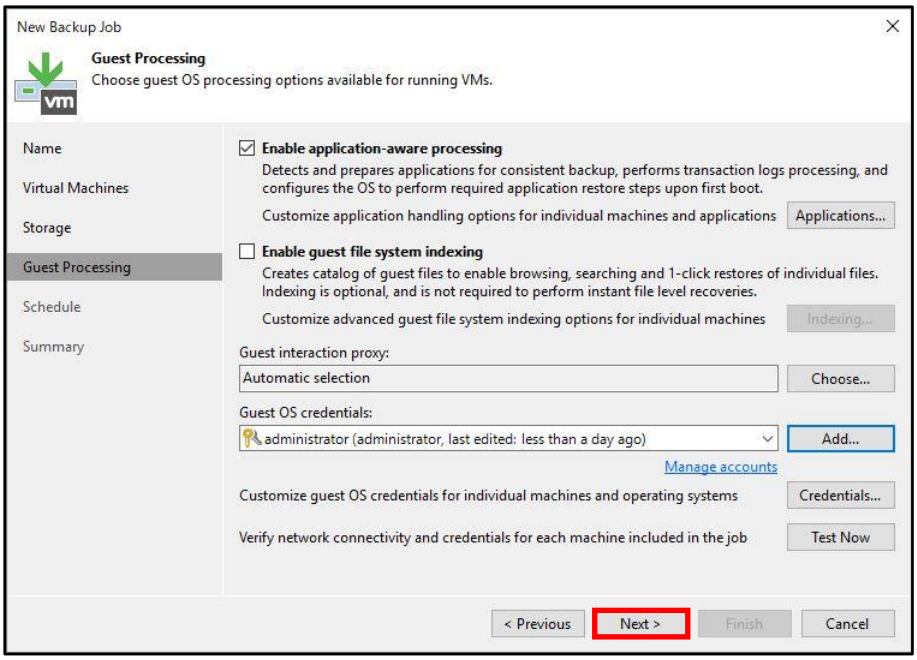
11. [Add...]-[Standard account...]をクリックします。



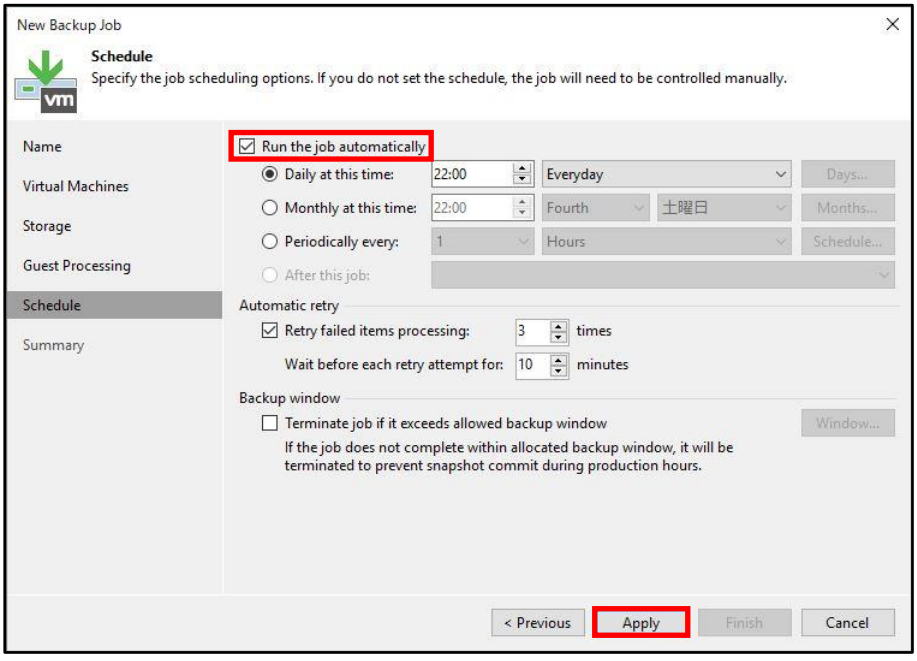
12. バックアップ対象の管理者アカウントとパスワードを入力して、[OK]をクリックします。
※本書では、[administrator]を使用します。



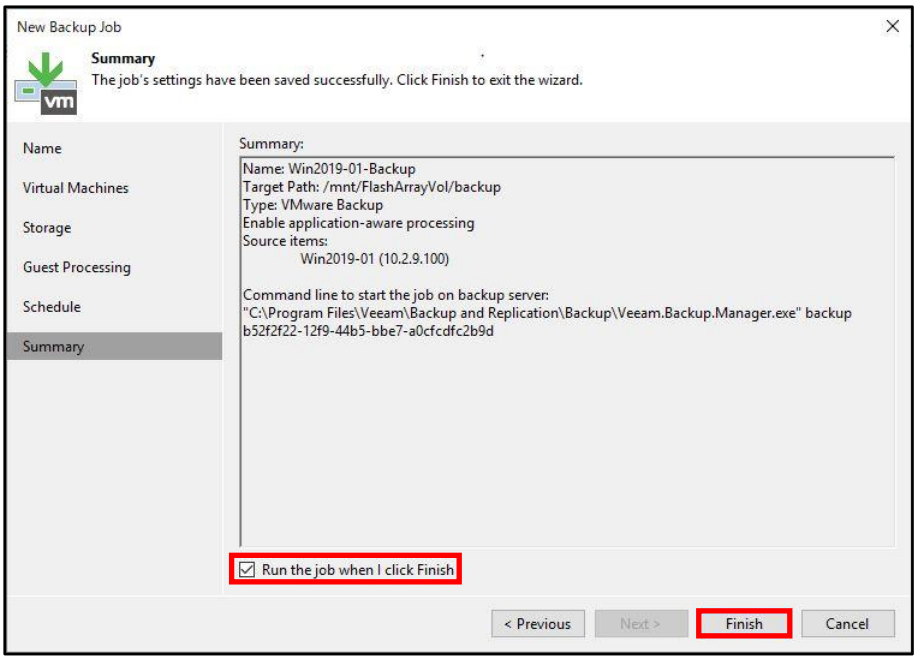
13. [Next >]をクリックします。



14. [Run the job automatically]にチェックを入れて、[Apply]をクリックします。
※本書では、デフォルトの毎日 22:00 を選択しています。



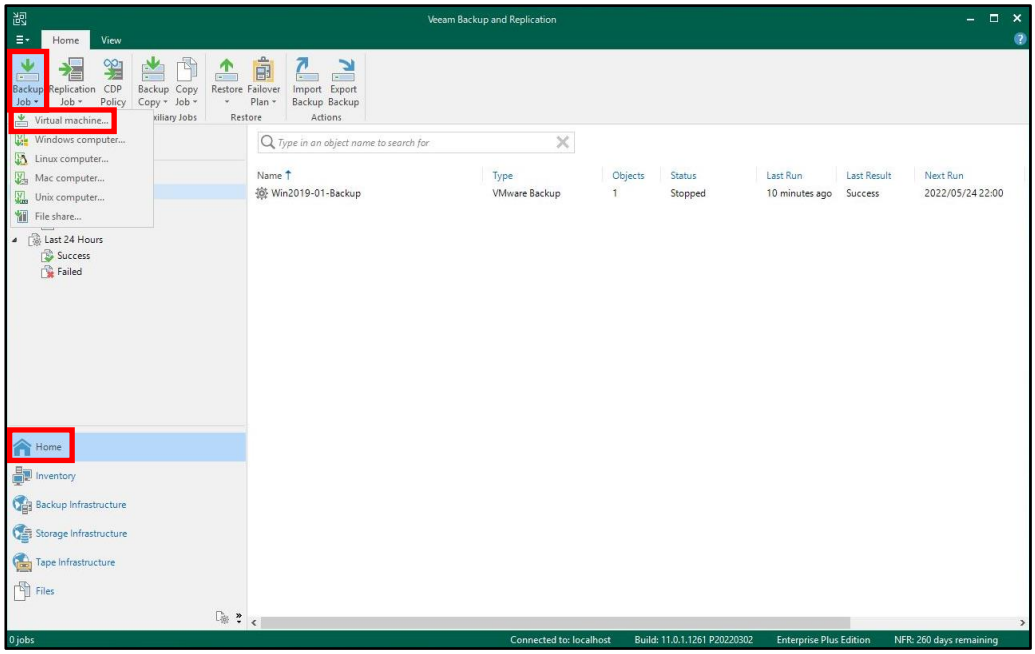
15. 本書ではジョブ作成後にジョブを即時実行しますので、[Run the job when I click Finish]にチェックを入れて[Finish]をクリックします。



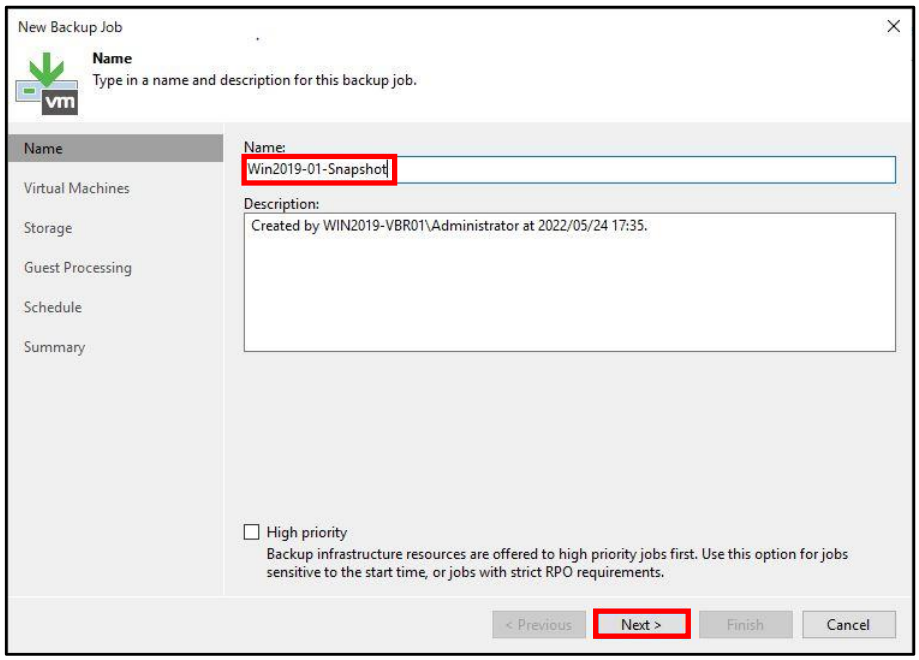
以上でストレージスナップショットを使用したバックアップ設定は完了です。

6.2.2. スナップショットオーケストレーション

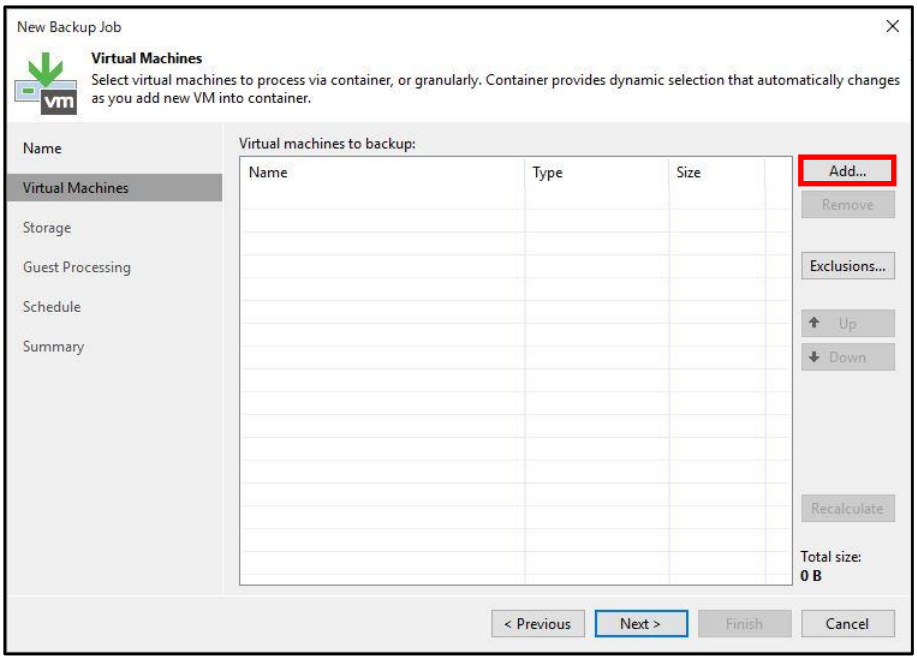
1. Veeam Backup & Replication Console の[HOME]-[Backup Job]-[Virtual machine...]をクリックします。



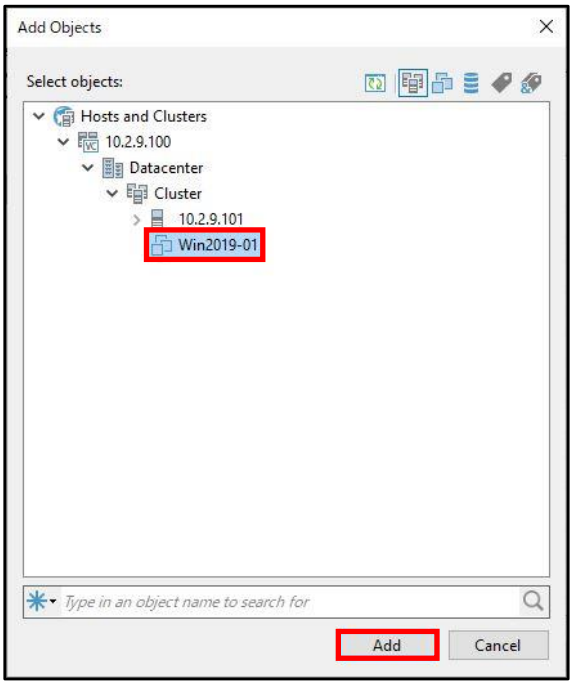
2. 任意のバックアップジョブ名を入力して、[Next >]をクリックします。



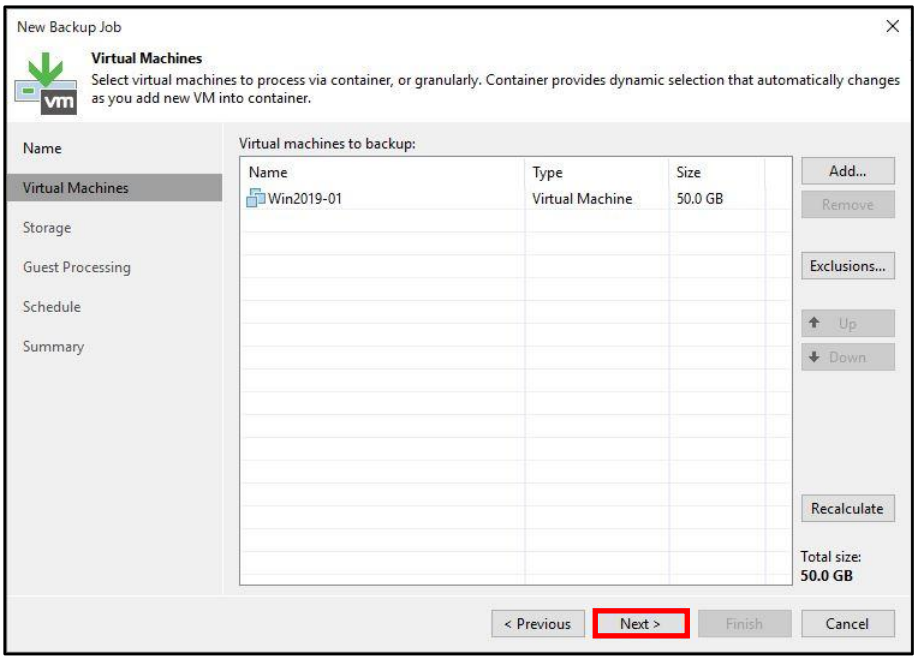
3. [Add...]をクリックします。



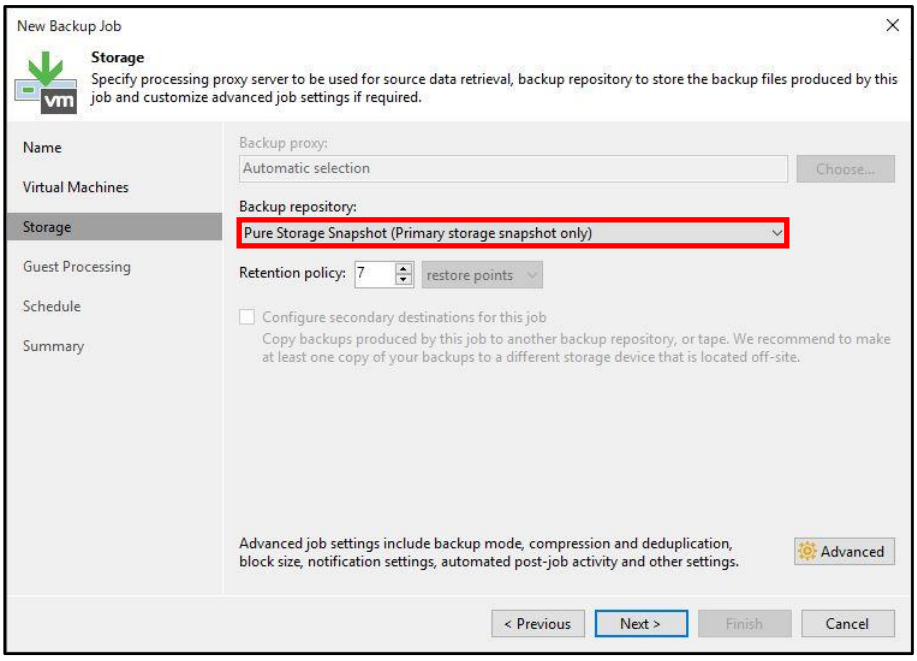
4. バックアップする仮想マシンを選択して、[Add]をクリックします。



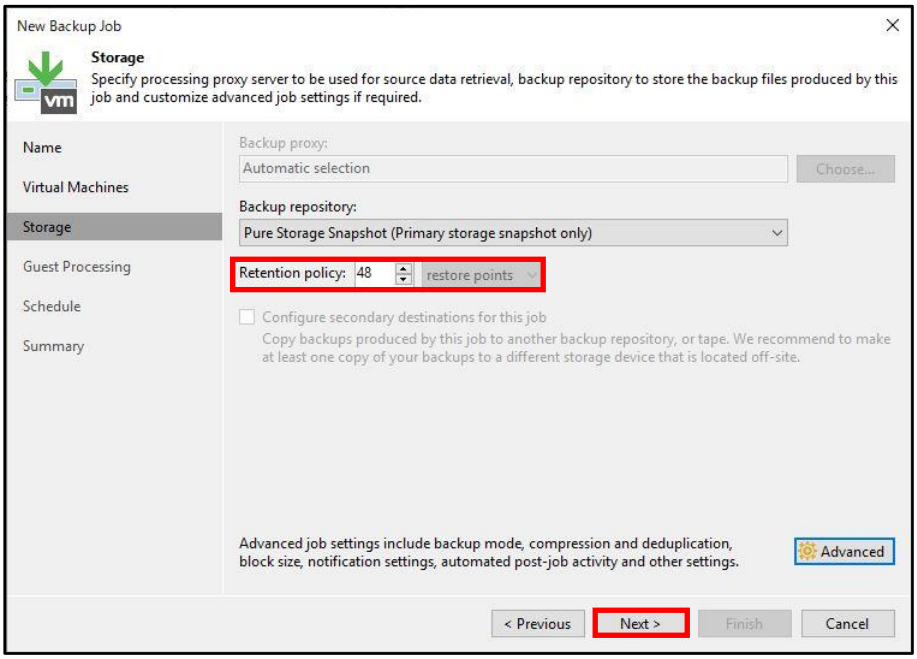
5. [Next >]をクリックします。



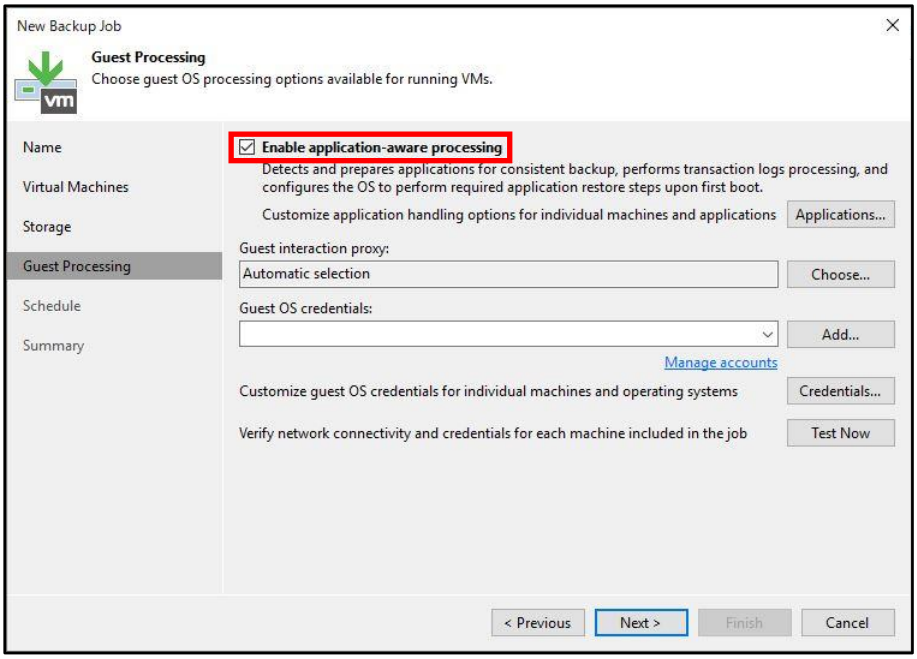
6. [Pure Storage Snapshot (Primary storage snapshot only)]を選択します。
※通常はバックアップレポジトリが表示されますが、ストレージ連携可能な機器を登録するとここでスナップショットが指定可能となります。



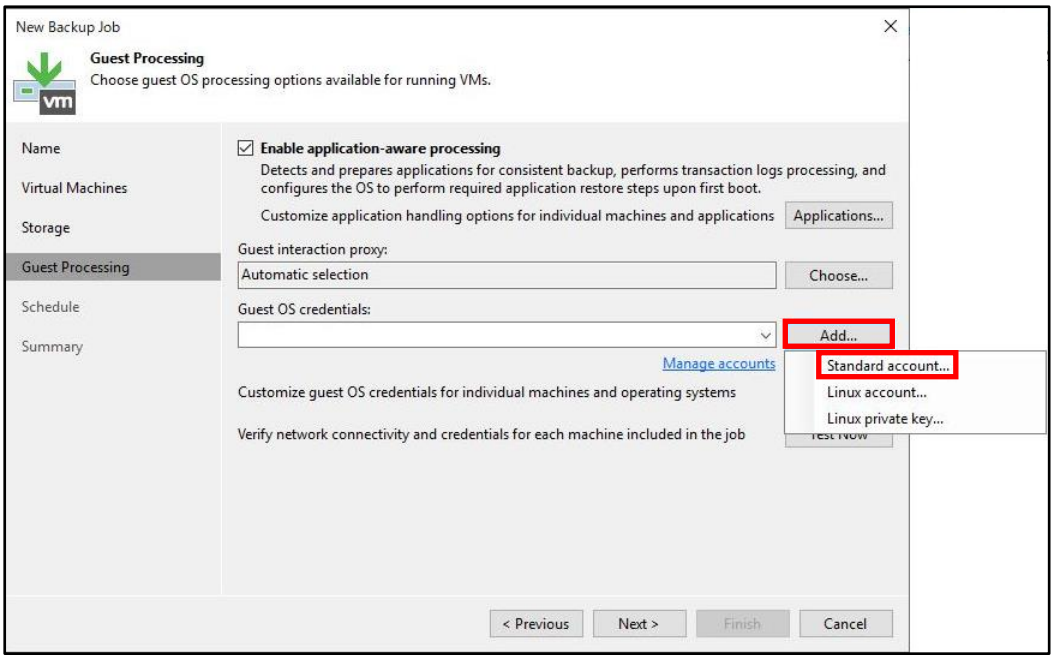
7. [Retention policy]を指定して、[Next >]をクリックします。
※[Retention policy]は、Pure Storage の Eradicate 操作不可期間に最低でも 1 日以上加えた設定になるように指定します。



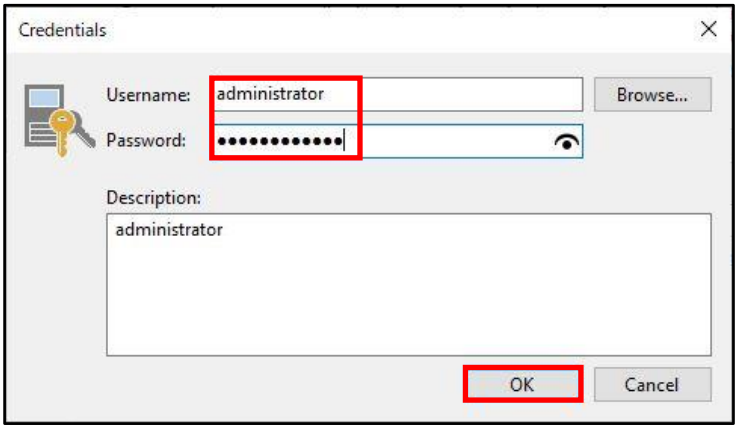
8. [Enable application-aware processing]にチェックを入れます。



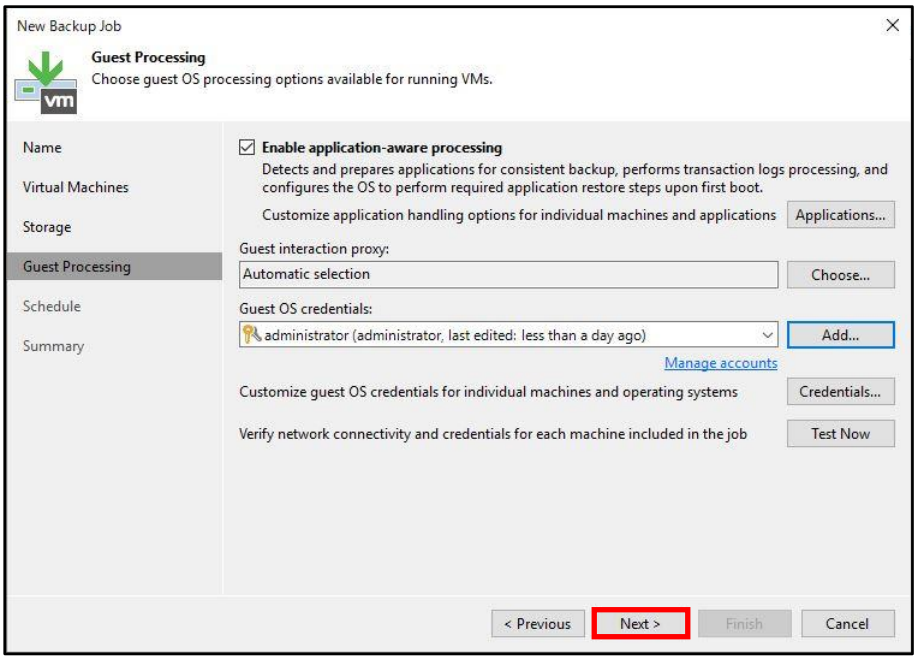
9. [Add...]-[Standard account...]をクリックします。



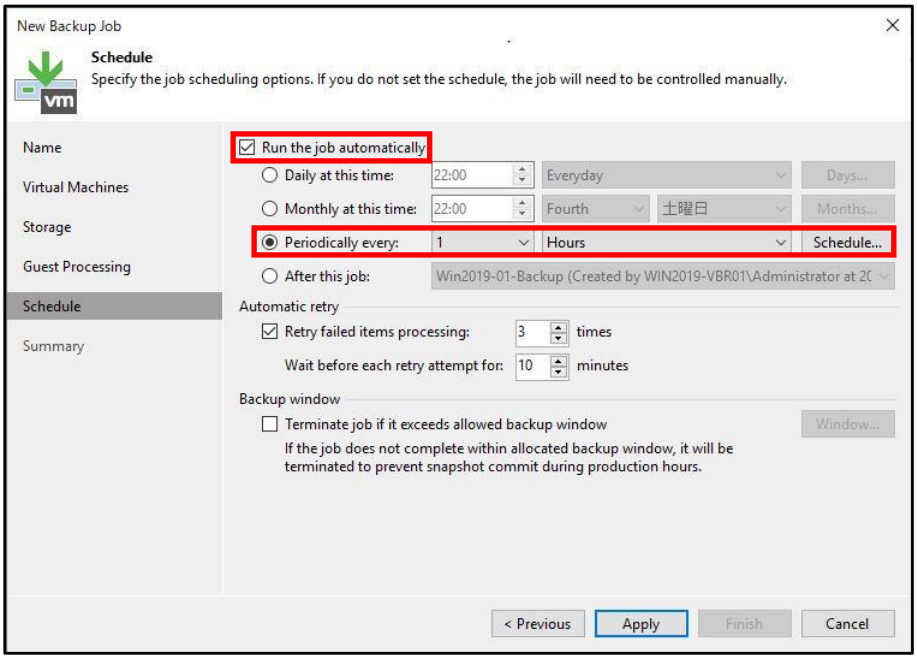
10. バックアップ対象の管理者アカウントとパスワードを入力して、[OK]をクリックします。
※本書では、[administrator]を使用します。



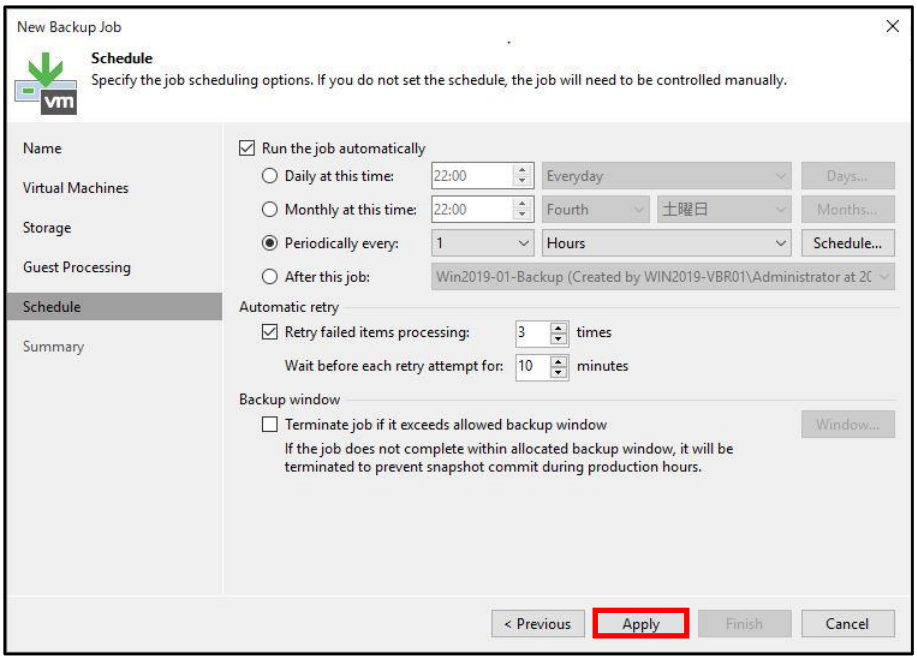
11. [Next >]をクリックします。



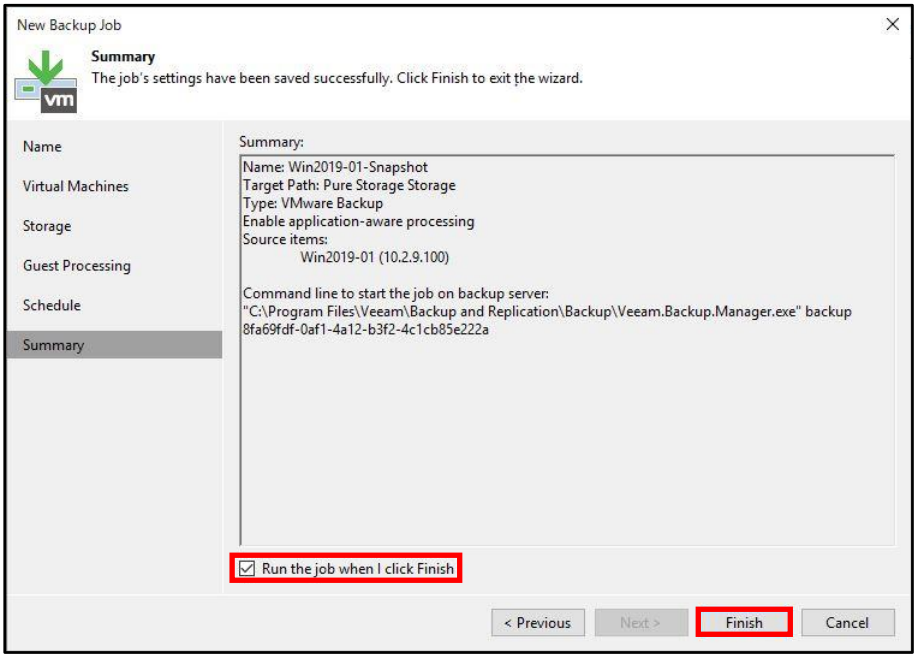
12. [Run the job automatically]にチェックを入れて、[Periodically every]を選択します。
※本書では、デフォルトの[1][Hours]を選択しています。



13. [Apply]をクリックします。



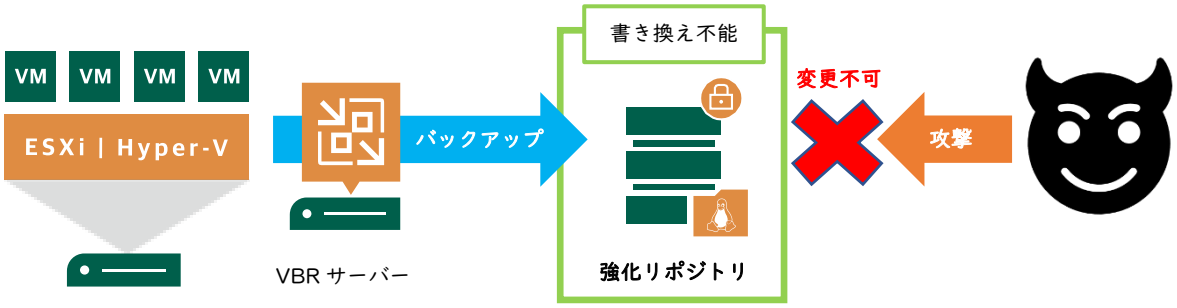
14. 本書ではジョブ作成後にジョブを即時実行しますので、[Run the job when I click Finish]にチェックを入れて[Finish]をクリックします。



以上でスナップショットオーケストレーションは完了です。

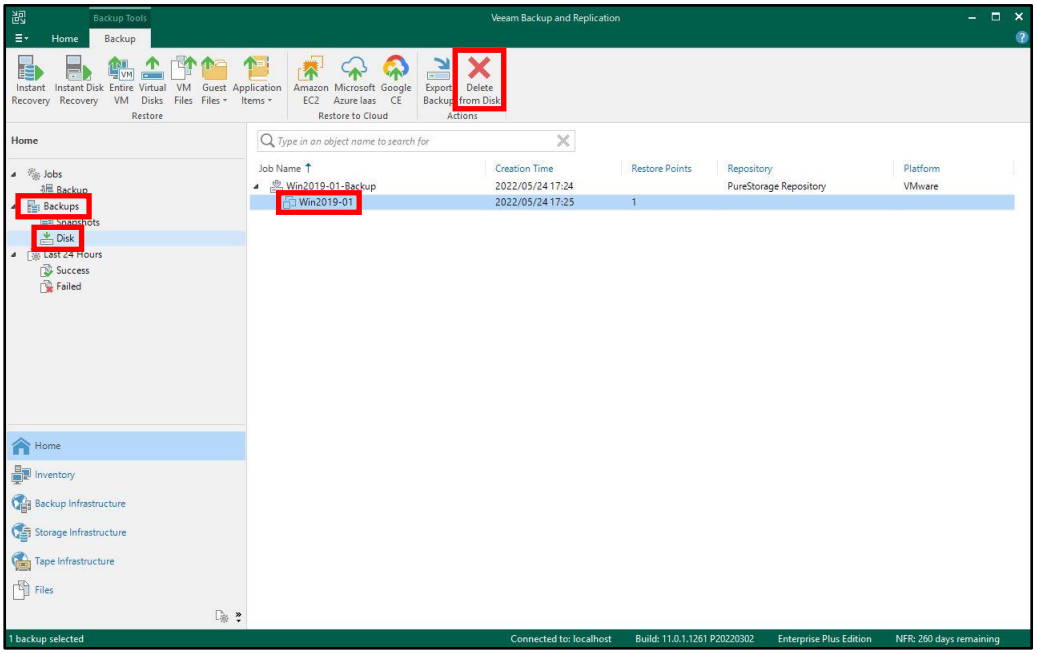
6.3. 強化(書き換え不能)Linux リポジトリの確認

強化（書き換え不能）Linux リポジトリは、バックアップデータを書き換え不能にできる機能です。併せて SSH によるリモートアクセスを遮断することが可能です。この機能を使用することで、バックアップデータが Immutable(不変的)なものとなり、悪意のある外部からの攻撃からバックアップデータを守ることができるだけでなく、外部侵入自体を防ぐことが可能です。

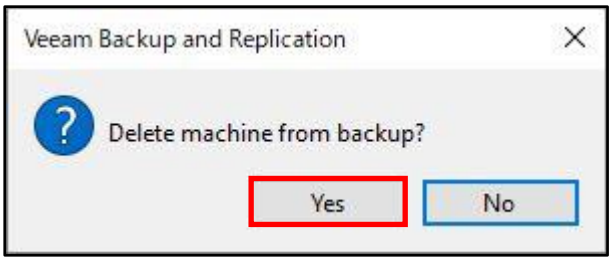


本書では、Veeam Backup & Replication のバックアップ管理者アカウントで強化（書き換え不能）Linux リポジトリ上のバックアップデータを削除できないことを確認します。

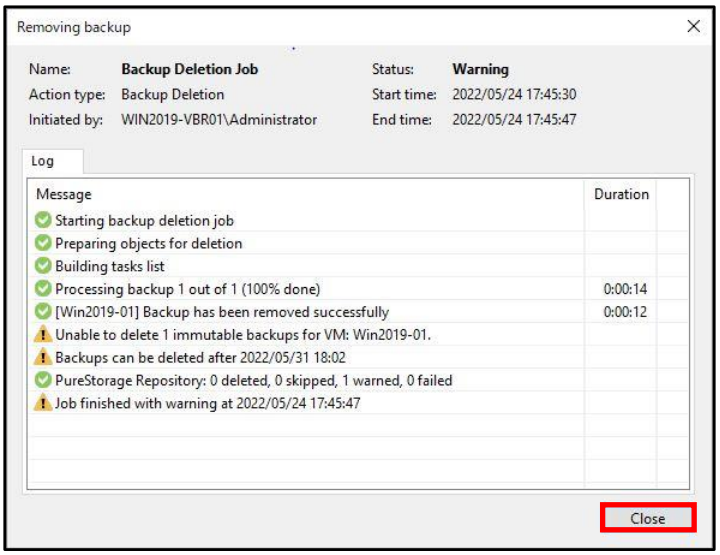
1. 書き換え不能なバックアップデータの確認のため[Backups]-[Disk]からバックアップデータを選択して、[Delete from Disk]をクリックします。



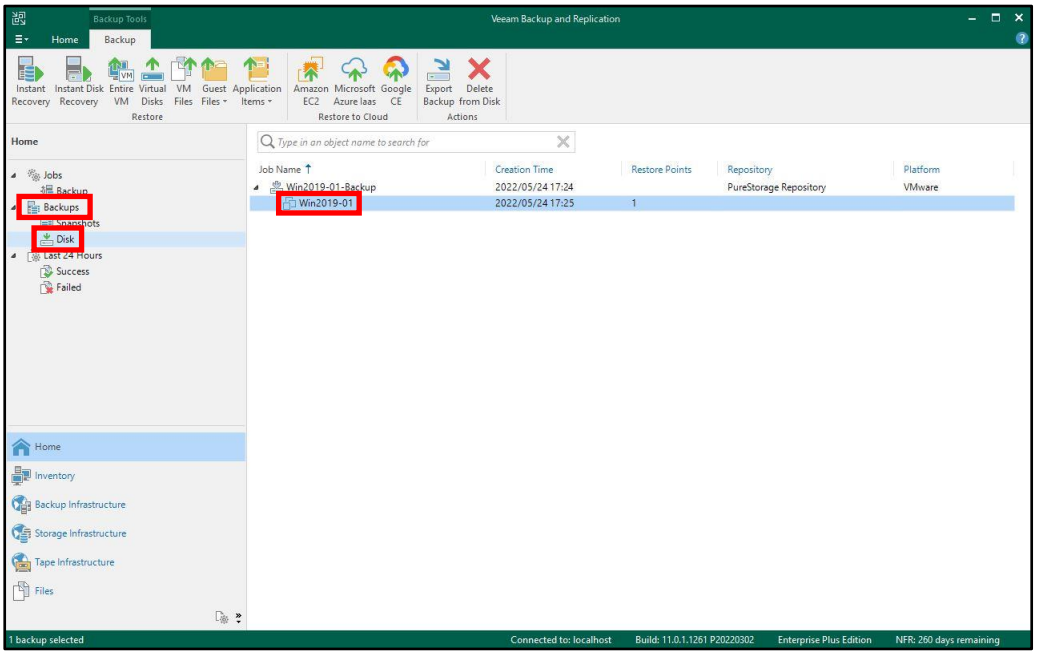
2. [Yes]をクリックします。



3. Warning で終了しますので、そのまま[Close]をクリックします。



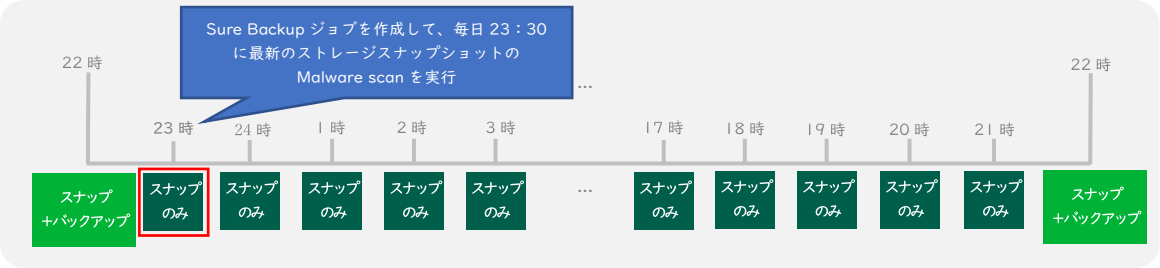
4. [Backups]- [Disk]をクリックします。
バックアップ管理者アカウントでもバックアップデータが削除できないことが確認できます。



以上で強化（書き換え不能）Linux リポジトリの確認は完了です。

6.4. SureBackup

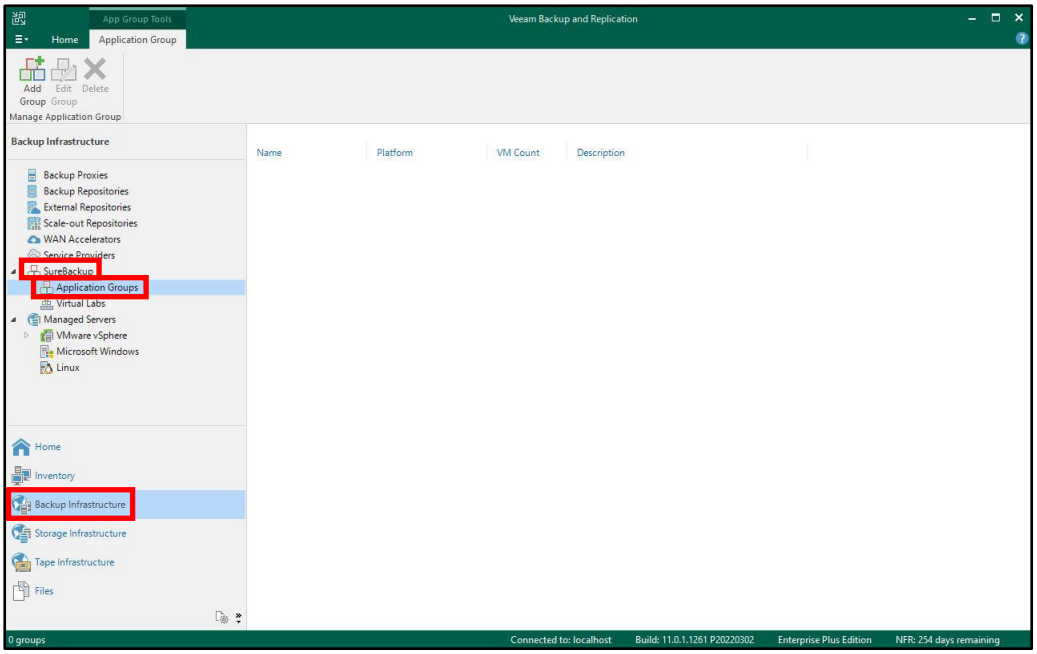
SureBackup は、あらゆるバックアップやレプリカ、スナップショットのリストアを自動的に検証することで、リストア関連の操作を向上させます。 また、マルウエアに対するバックアップのスキャン操作の自動化によって、ランサムウエアを阻止しリストアの安全性を確保します。



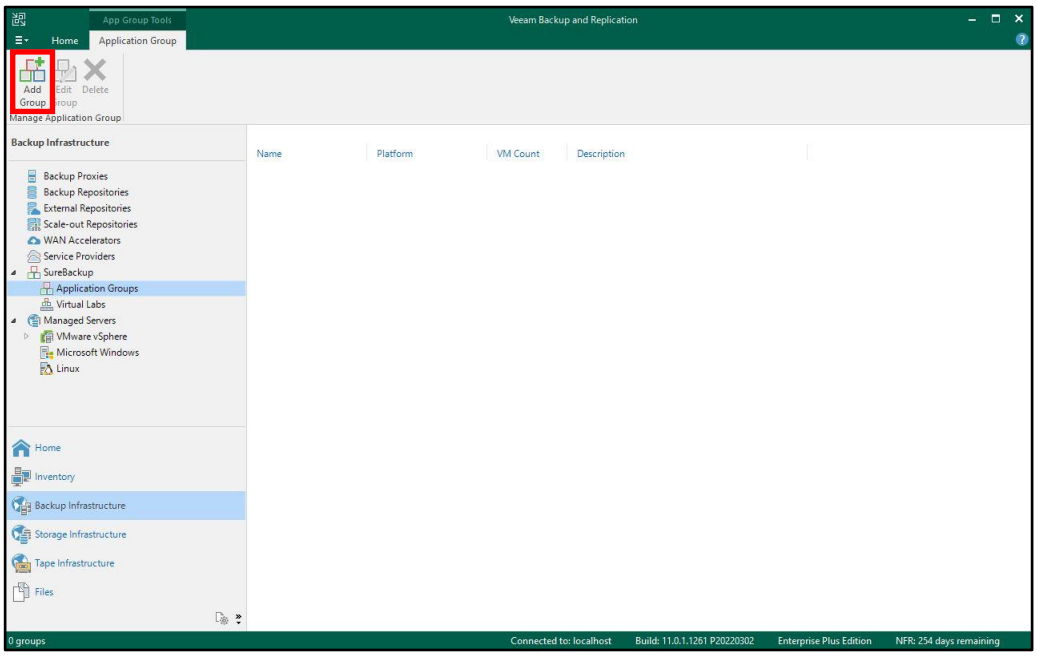
本書では、Application Group と Virtual Lab の作成、SureBackup ジョブを作成して定期的（毎日 23:30）に Application Group を Malware scan する手順を説明します。

6.4.1. Application Group の作成

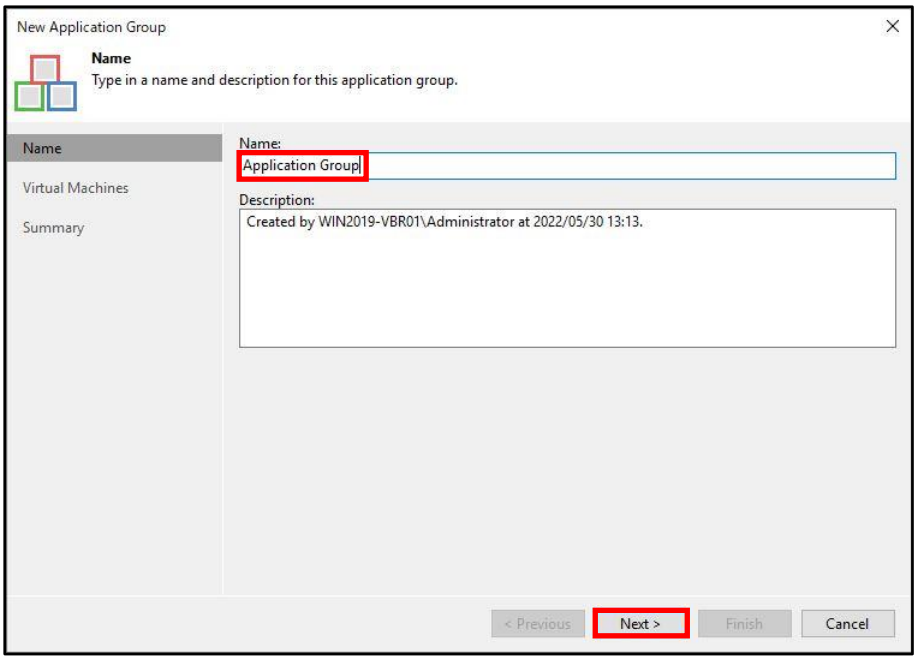
1. Veeam Backup & Replication Console の [Backup Infrastructure]-[Sure Backup]-[Application Groups]をクリックします。



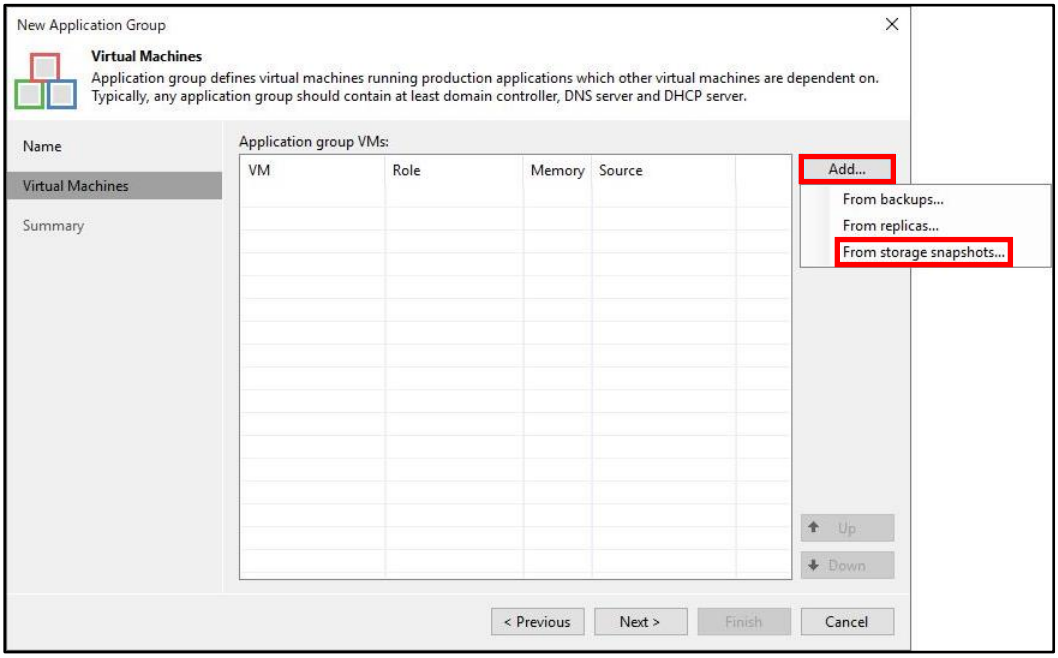
2. [Add Group]をクリックします。



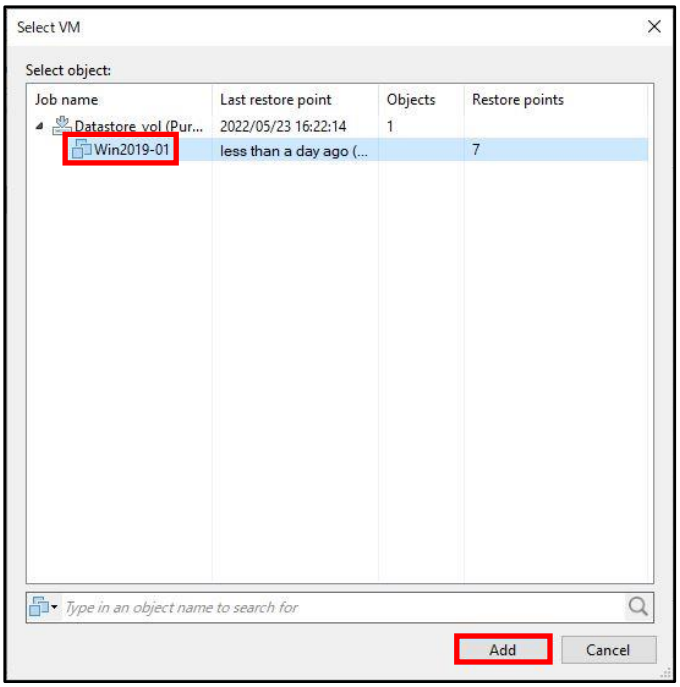
3. 任意のグループ名を入力して、[Next >]をクリックします。
※本書では、[Application Group]としています。



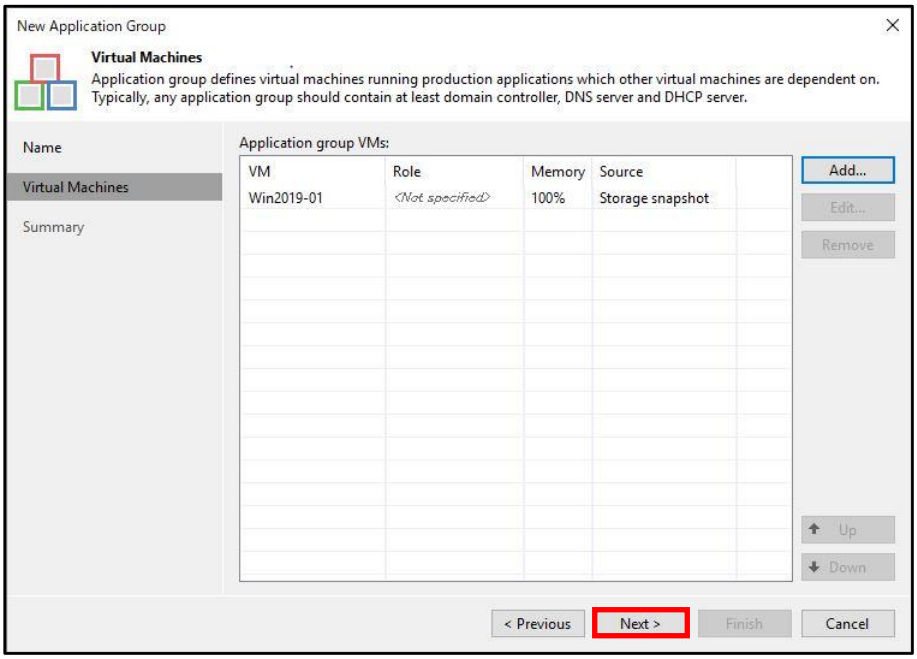
4. [Add...]-[From storage snapshots...]をクリックします。



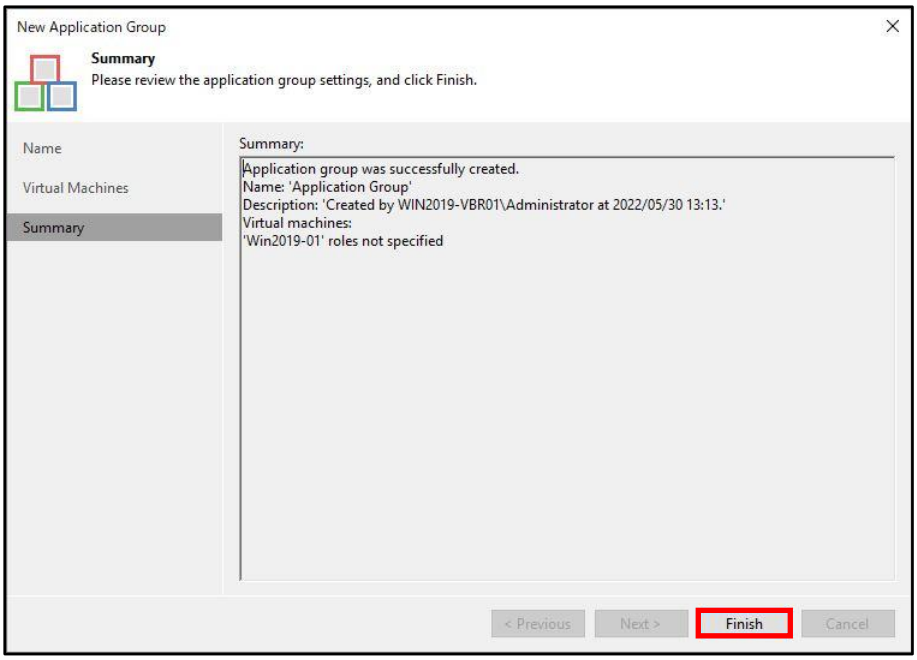
5. グループに含む仮想マシンを選択して、[Add]をクリックします。



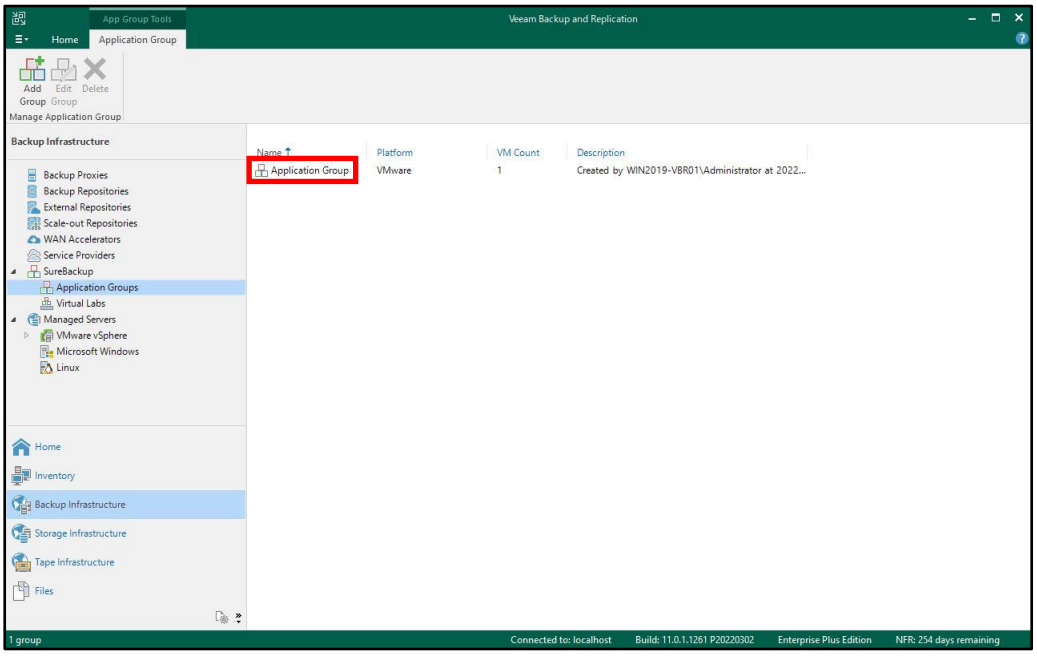
6. 仮想マシンが追加されたことを確認して、[Next >]をクリックします。
※本書では実施しませんが、Verification Options で詳細な設定をする場合は仮想マシンを選択して[Edit]をクリックします。



7. [Finish]をクリックします。



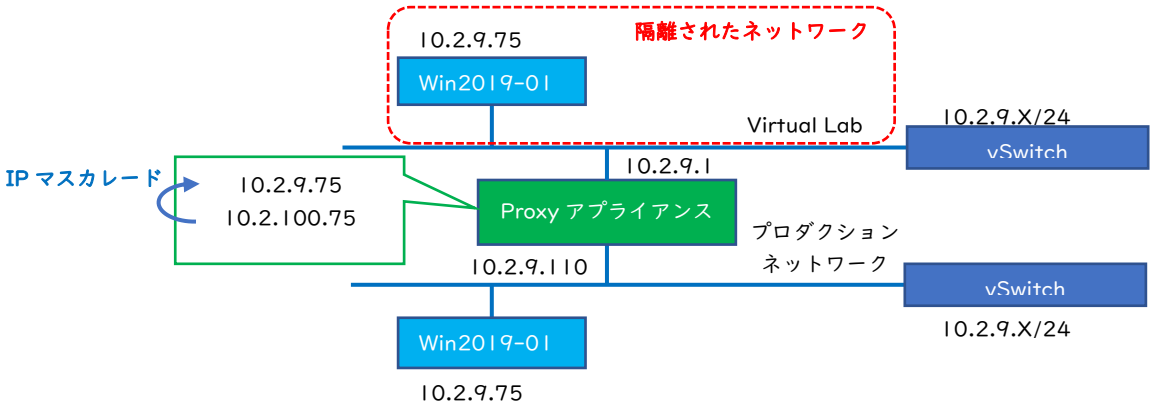
8. グループが追加されたことを確認します。



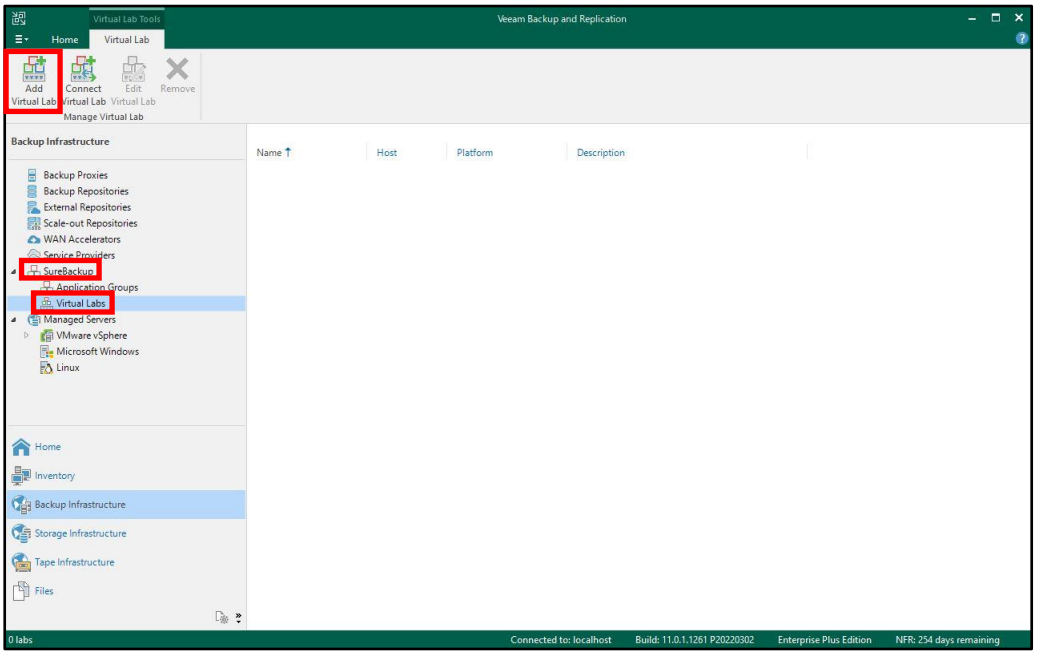
以上で Application Group の作成は完了です。

6.4.2. Virtual Lab の作成

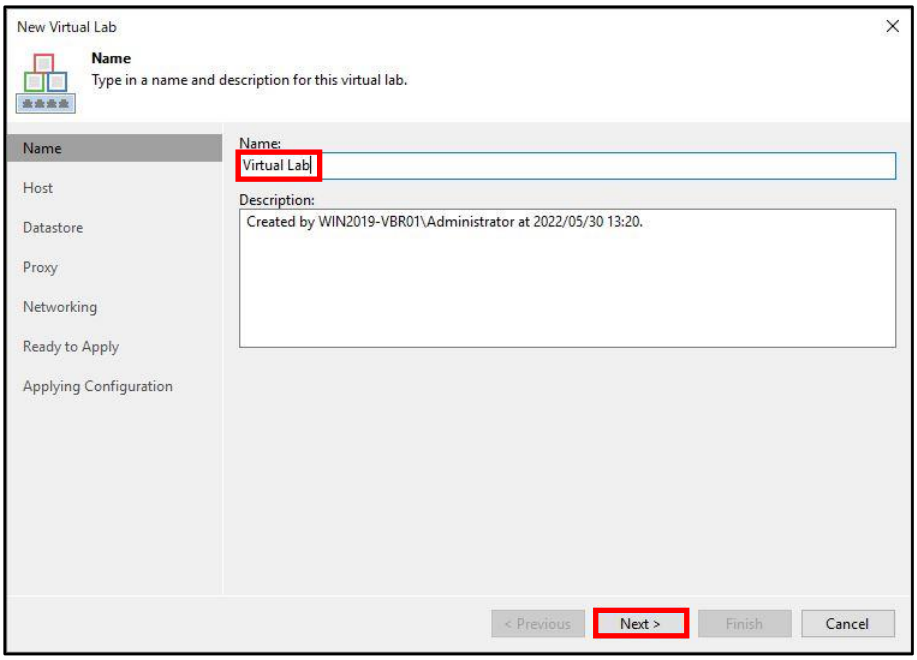
本書では、下記の構成となるように Virtual Lab を作成します。



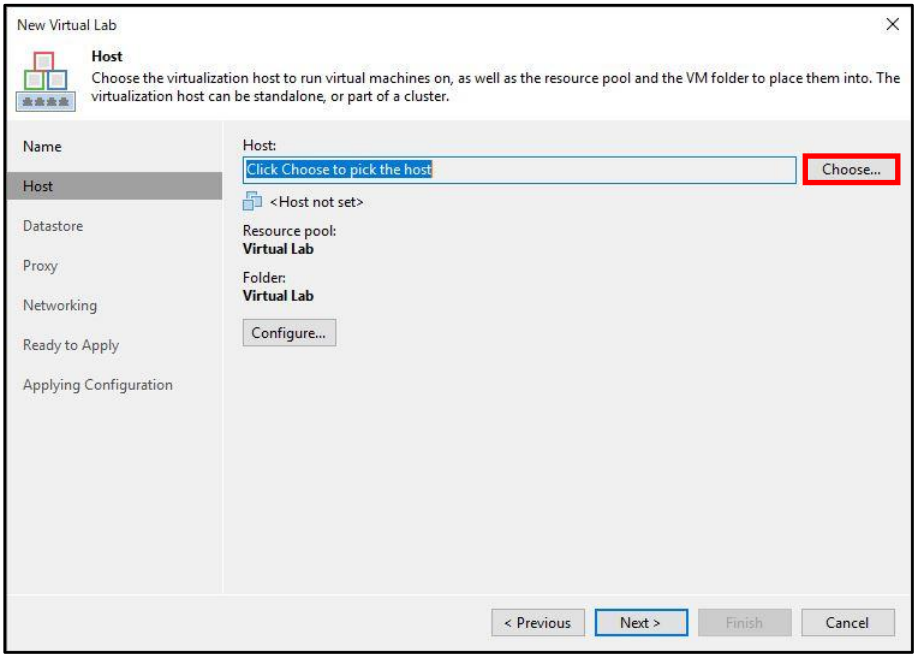
1. Veeam Backup & Replication Console の[Sure Backup]-[Virtual Labs]- [Add Virtual Lab]をクリックします。



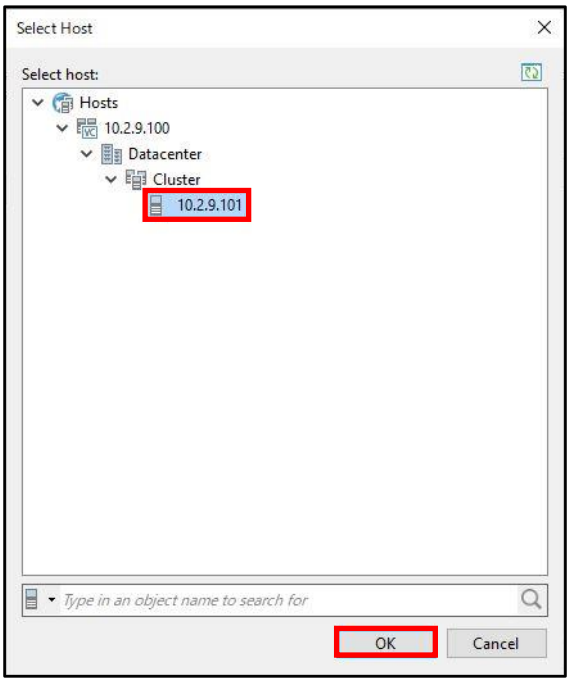
2. 任意の Virtual Lab 名を入力して、[Next >]をクリックします。
※本書では、[Virtual Lab]としています。



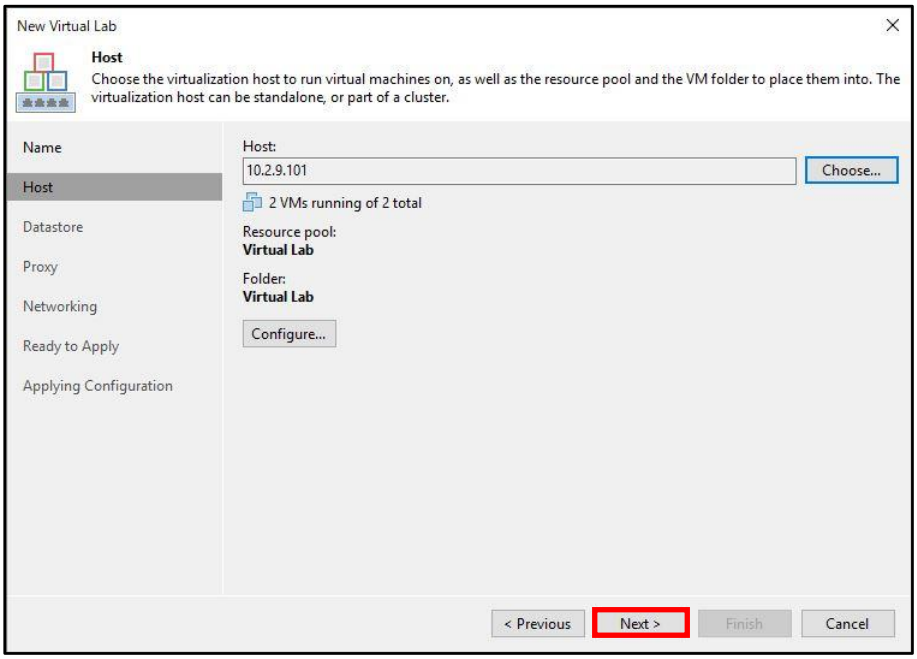
3. 仮想マシンを展開する VMware ESXi ホストを選択しますので、[Choose...]をクリックします。



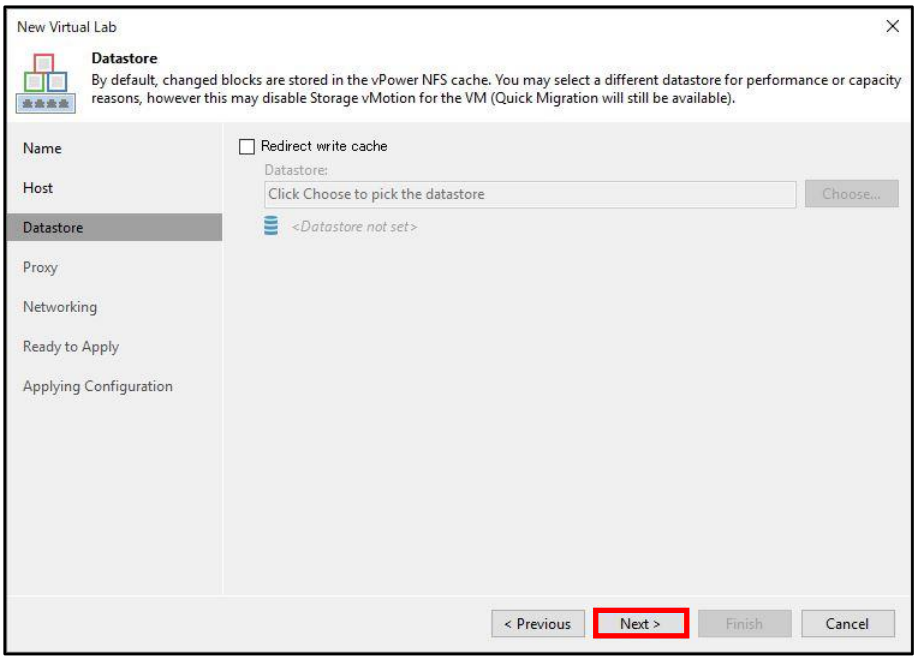
4. 仮想マシンを展開する ESXi ホストを選択して、[OK]をクリックします。



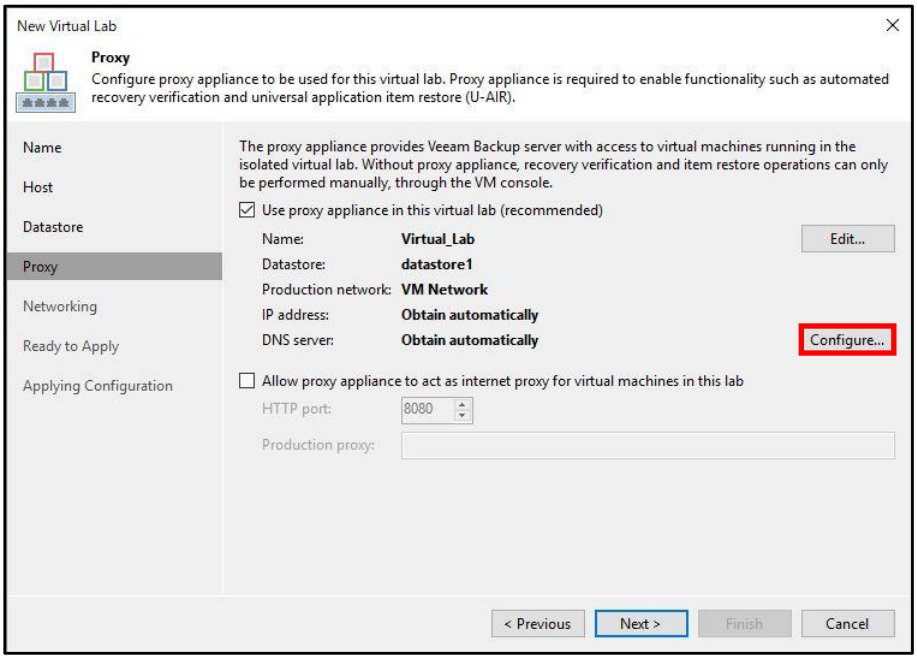
5. ESXi ホストが選択されたことを確認して、[Next >]をクリックします。
※仮想マシンはデフォルトでリソースプールとフォルダが Virtual Lab 名で新たに作成され展開されるので必要に応じて「Configure」をクリックしリソースプールとフォルダを変更してください。



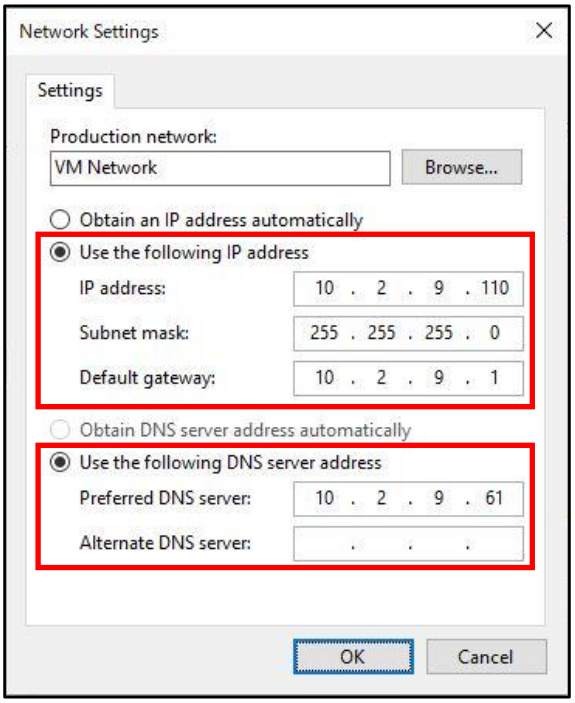
6. [Next >]をクリックします。



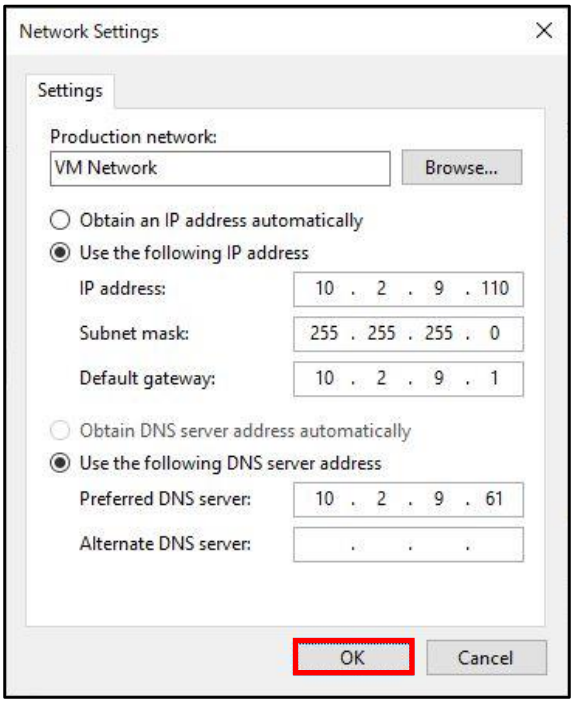
7. Proxy アプライアンスのネットワーク設定を行いますので、「Configure」をクリックします。



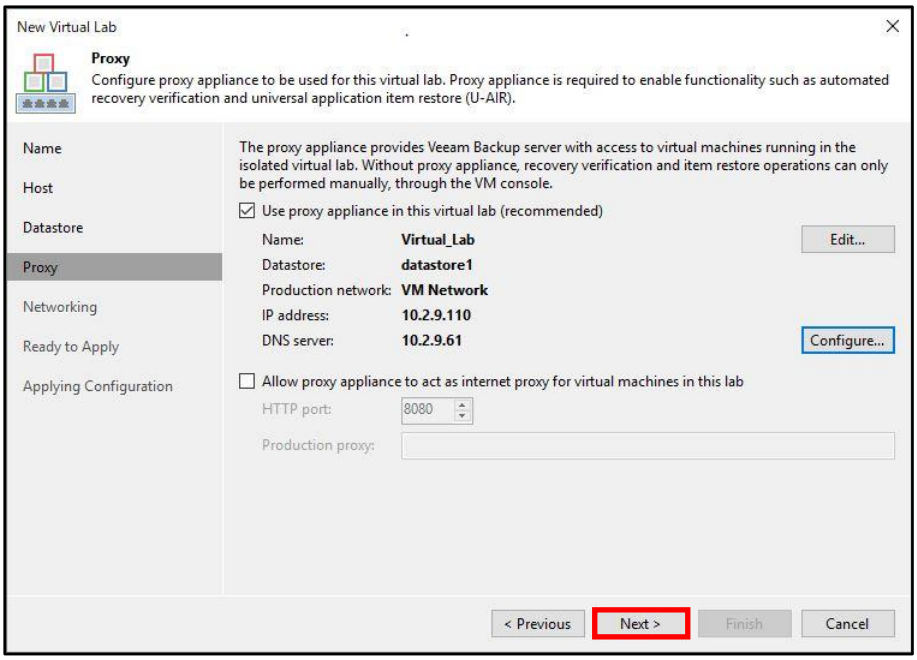
8. IP アドレスは Proxy アプライアンスがプロダクションネットワークに接続するための IP アドレスを入力します。 ※プロダクションネットワークとなる仮想スイッチを変更する場合は「Browse」をクリックします。



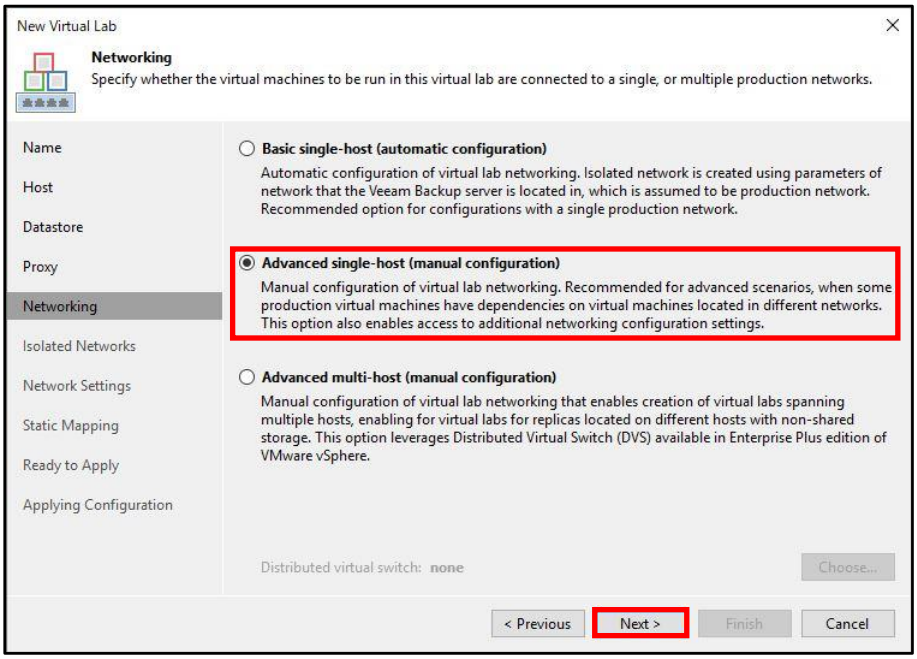
9. [OK]をクリックします。



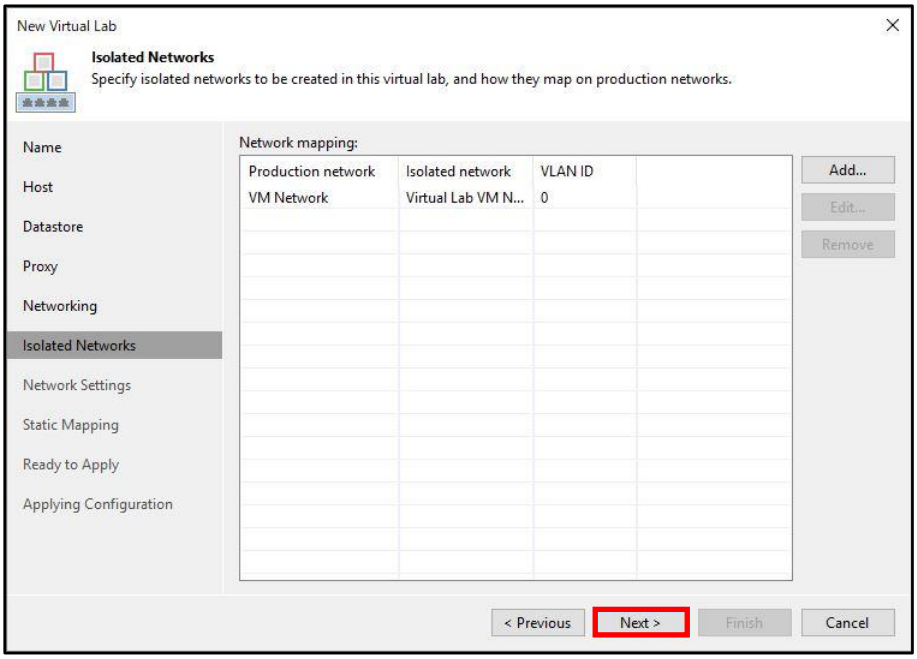
10. [Next >]をクリックします。



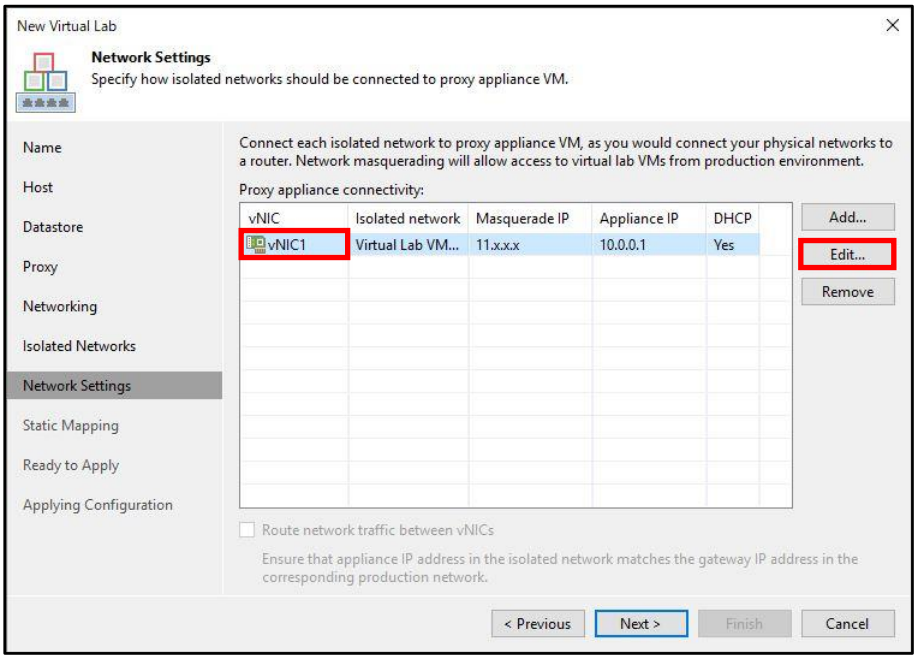
11. Virtual Lab のネットワーク設定を行いますので、「Advanced single-host (manual configuration)」を選択して「Next」をクリックします。



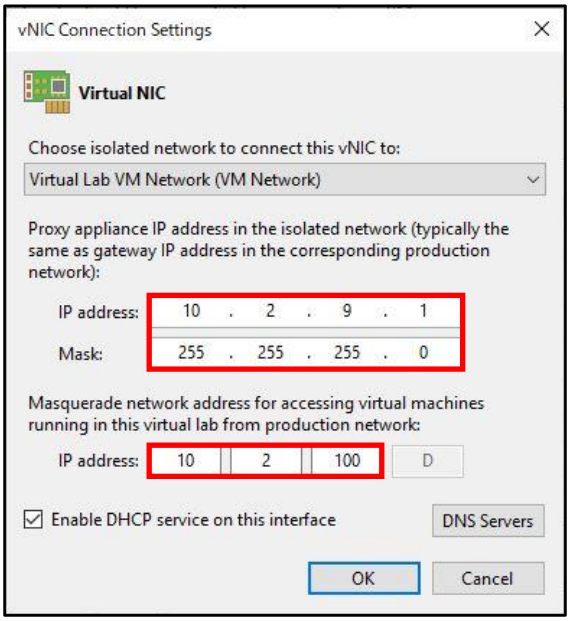
12. Virtual Lab で使用する隔離された vSwitch の設定を行います。 デフォルトでプロダクションネットワークの名前に合わせた vSwitch が作成されますので、本書ではそのまま[Next >]をクリックします。 ※変更する場合は「Edit」をクリックします。



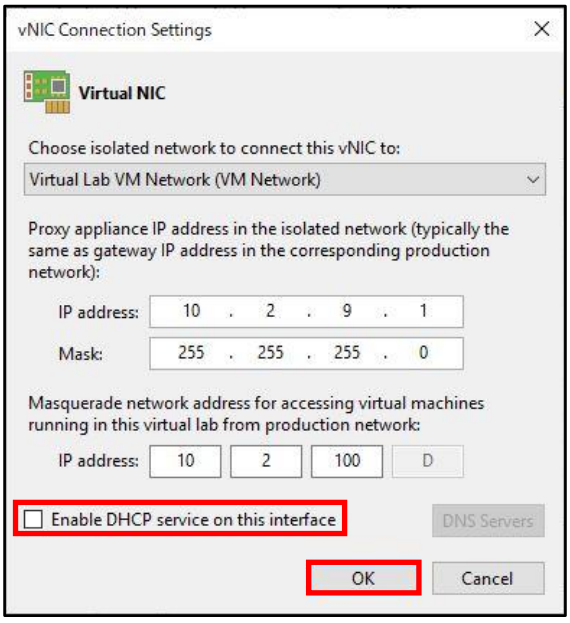
13. Proxy アプライアンスが接続する Virtual Lab のネットワークの設定を行いますので、[vNIC1]-[Edit...]をクリックします。



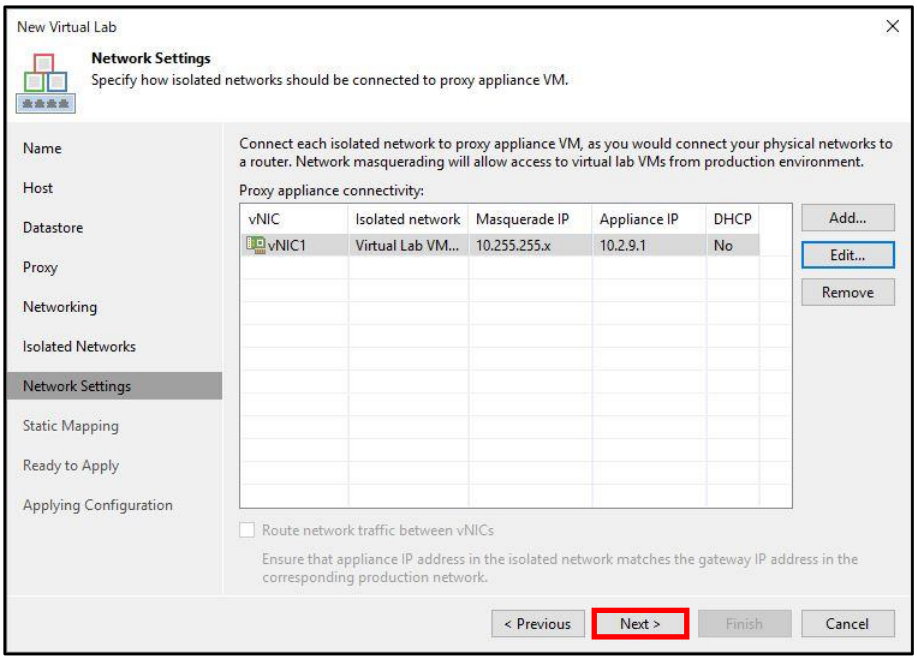
14. Proxy アプライアンスは Virtual Lab 内の仮想マシンから見るとルータの役割になっているため、設定する IP アドレスはデフォルトゲートウェイとして設定します。また、プロダクションネットワークから Virtual Lab にアクセスするための IP マスカレードで使用するサブネットも合わせて設定します。



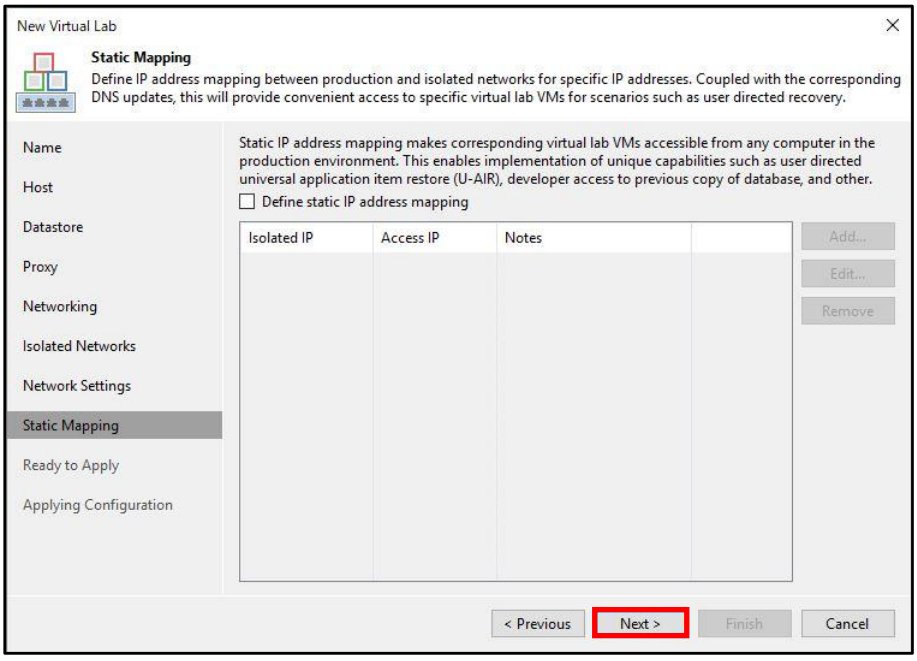
15. [Enable DHCP service on this interface]のチェックを外して、[OK]をクリックします。



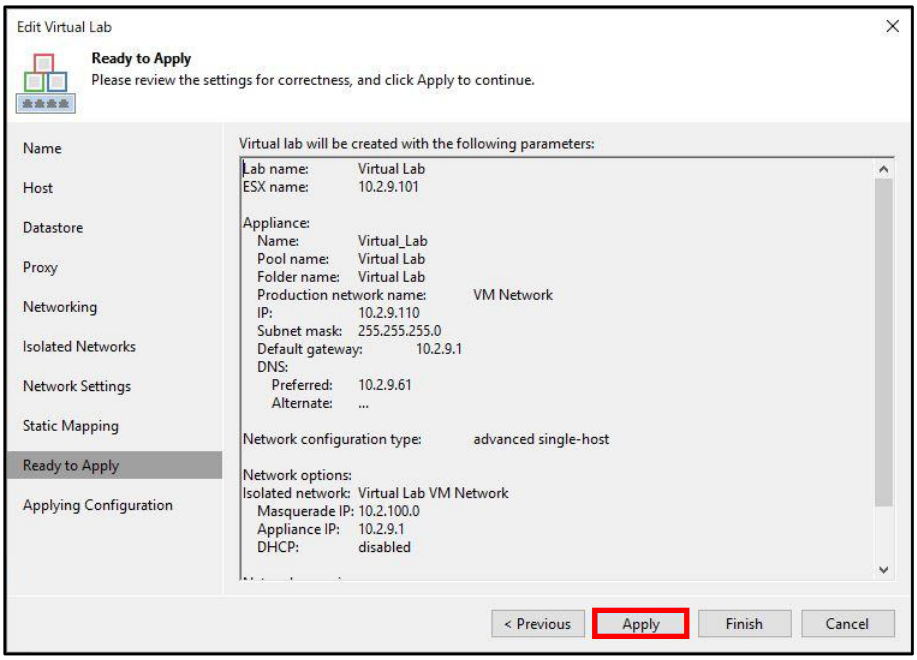
16. [Next >]をクリックします。



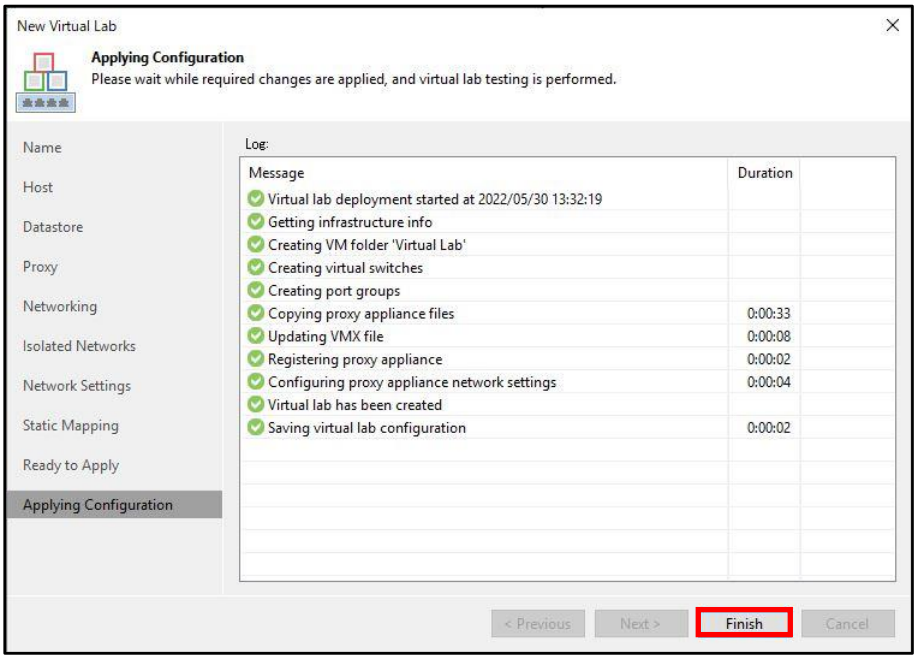
17. [Next >]をクリックします。



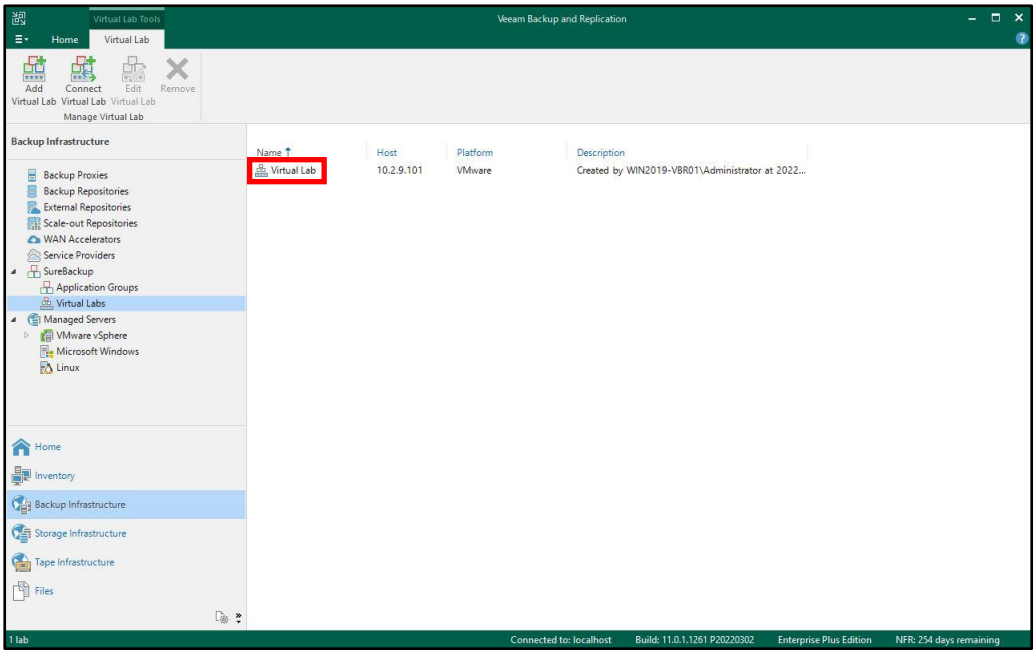
18. [Apply]をクリックします。



19. [Finish]をクリックします。



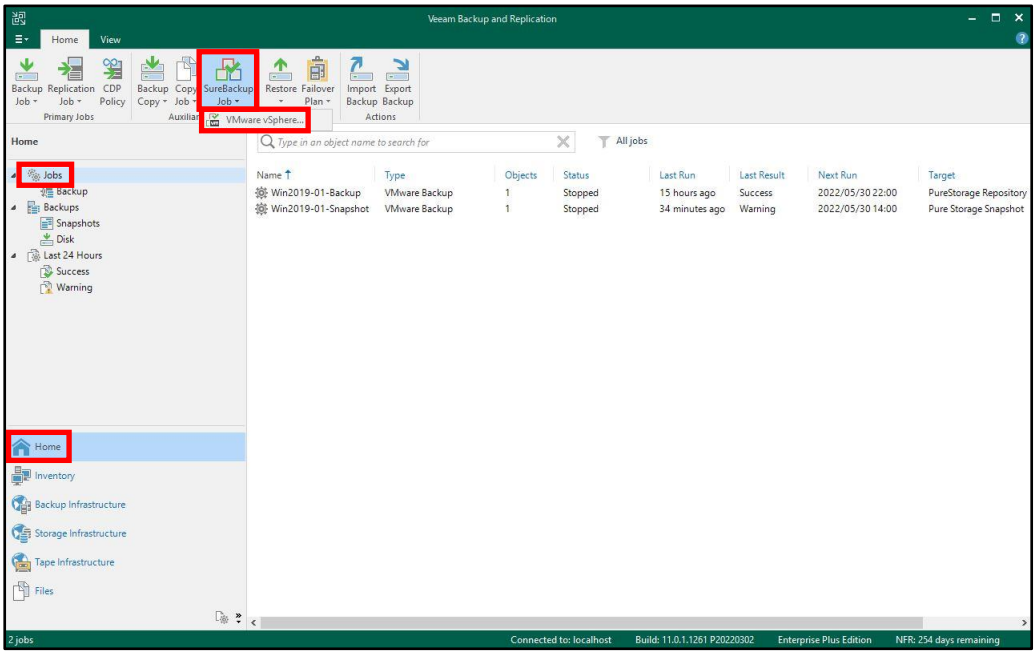
20. Virtual Lab が追加されたことを確認します。



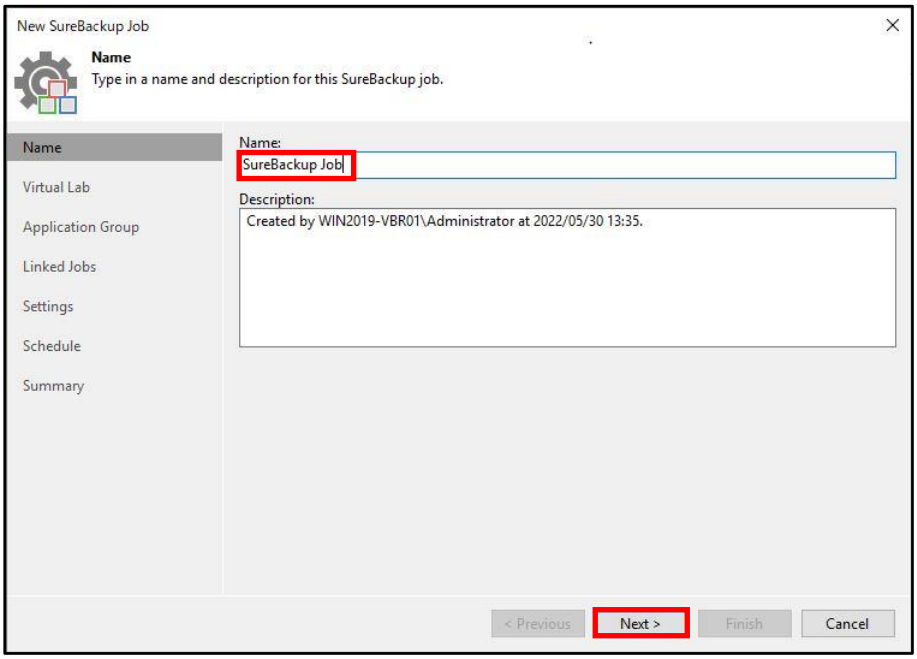
以上で Virtual Lab の作成は完了です。

6.4.3. SureBackup ジョブの作成と実行

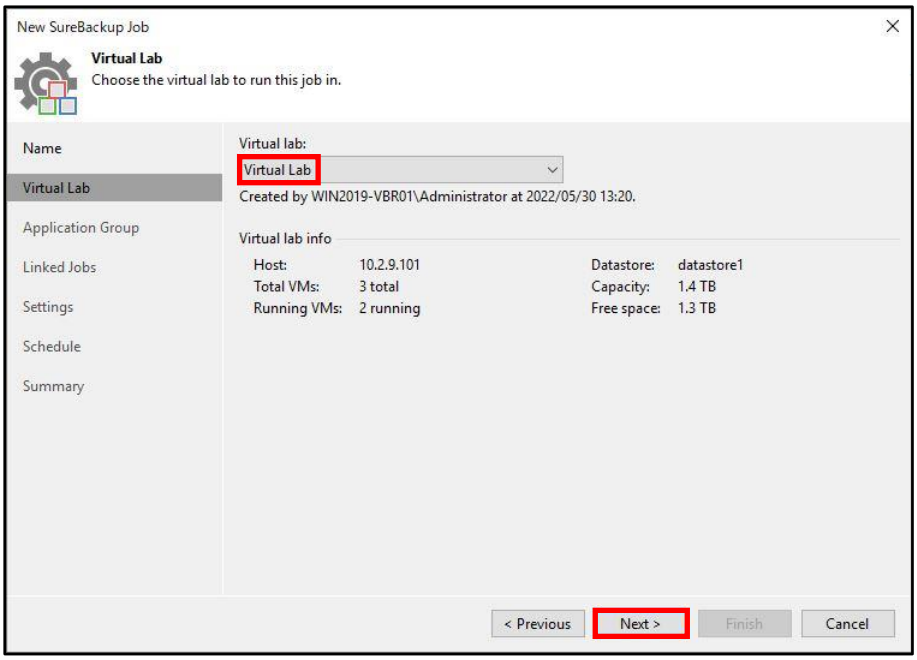
1. Veeam Backup & Replication Console の [Home]-[Jobs]-[SureBackup Job]-[VMware vSphere...]をクリックします。



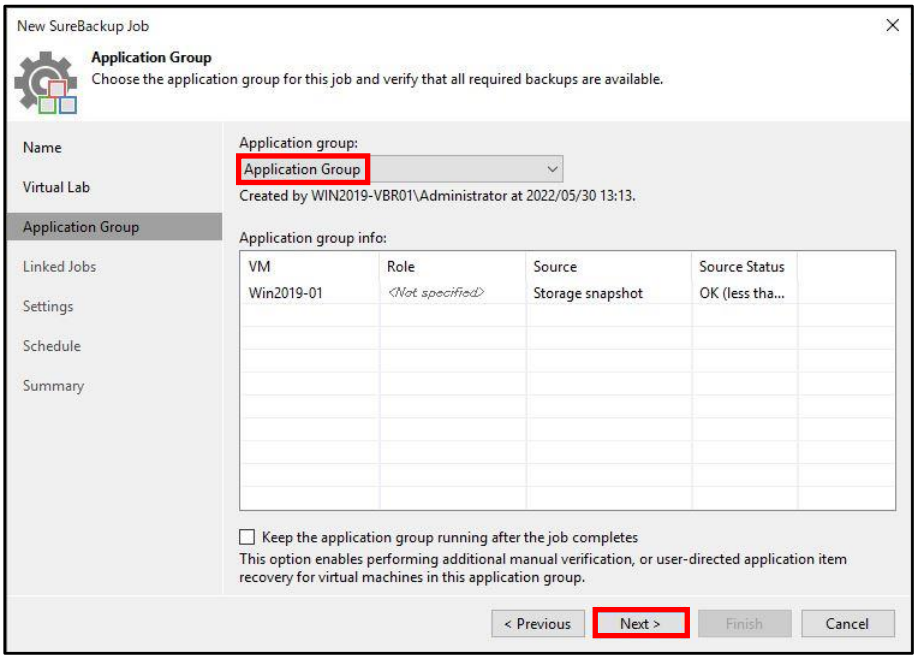
2. 任意の SureBackup ジョブ名を入力して、[Next >]をクリックします。



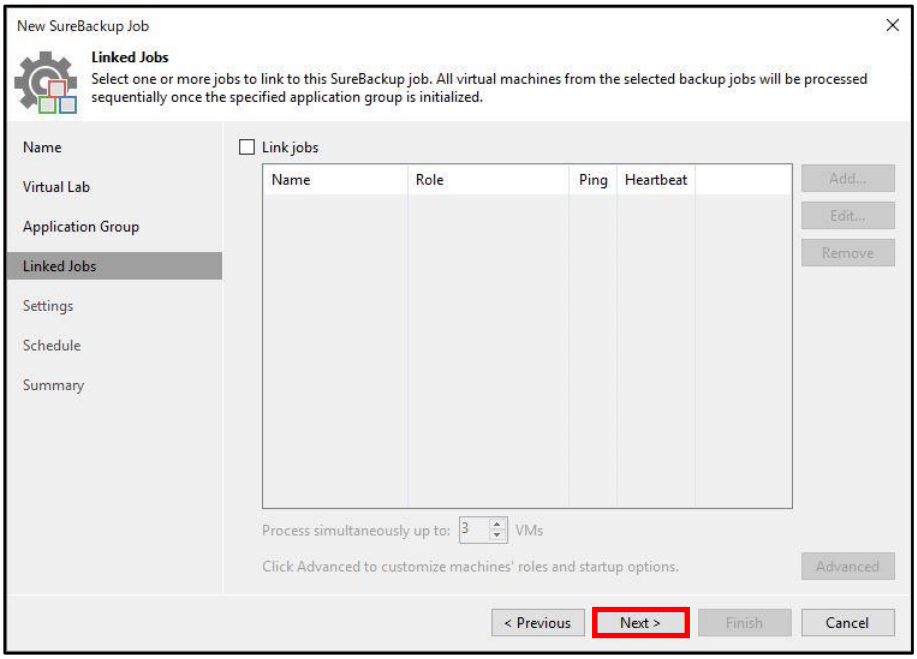
3. [Virtual Lab]の画面で作成した Virtual Lab を選択して、[Next >]をクリックします。



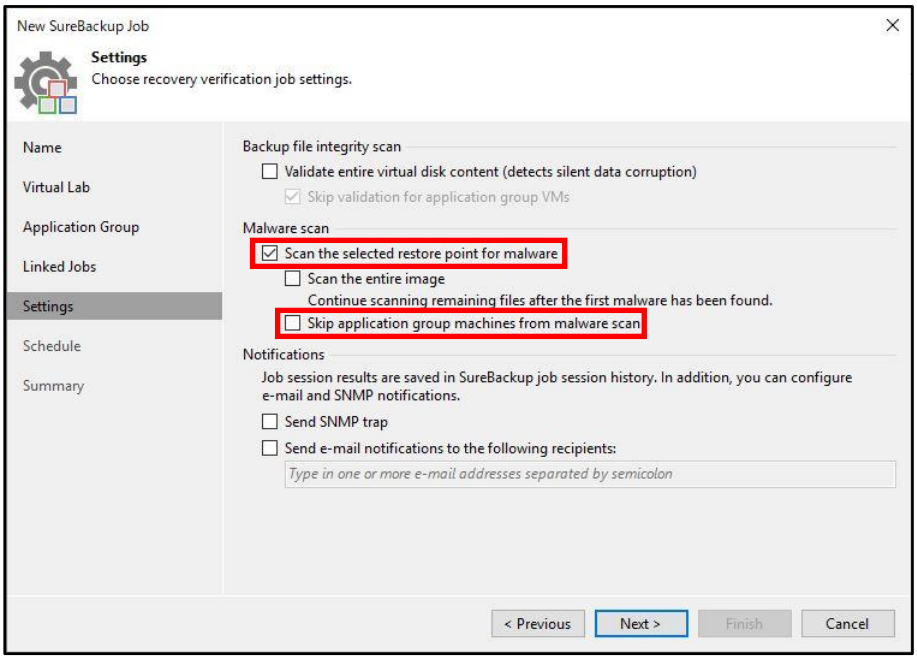
4. [Application Group]の画面で作成したアプリケーショングループを選択して、[Next >]をクリックします。



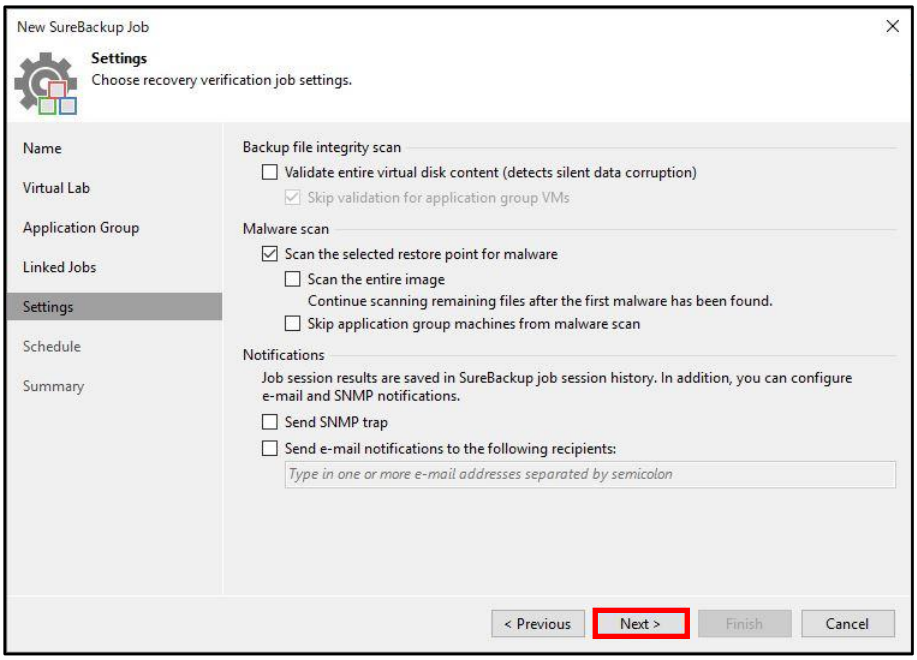
5. 本書では Application Group を Malware scan しますので、そのまま[Next >]をクリックします。



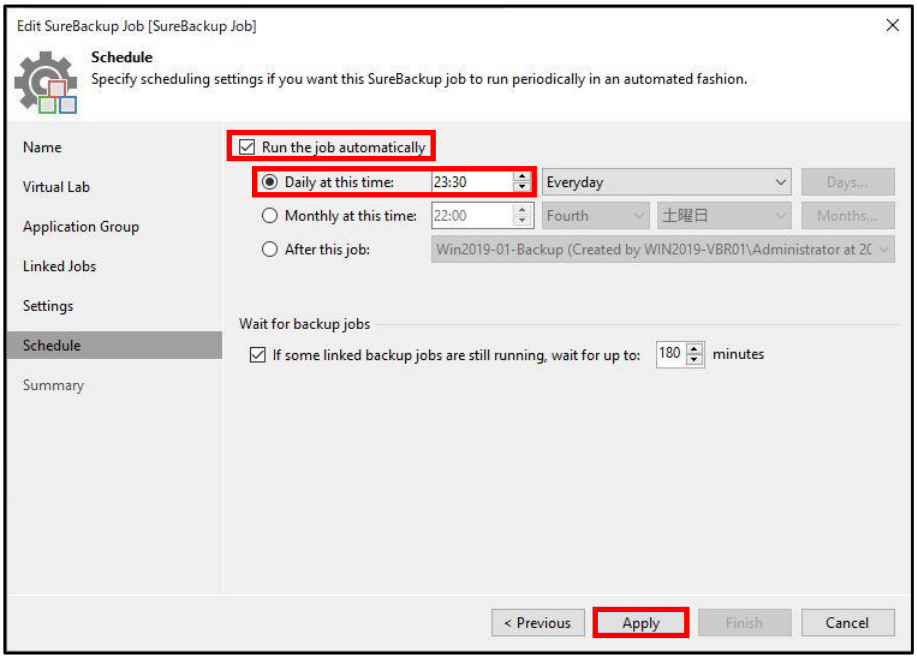
6. [Scan the selected restore point for malware]にチェックして、Application Group を Malware scan しますので[Skip application group machines from malware scan]のチェックを外します。
※最初のマルウエアが検出された後に Malware scan を続行する場合は、[Scan the entire image]にチェックします。



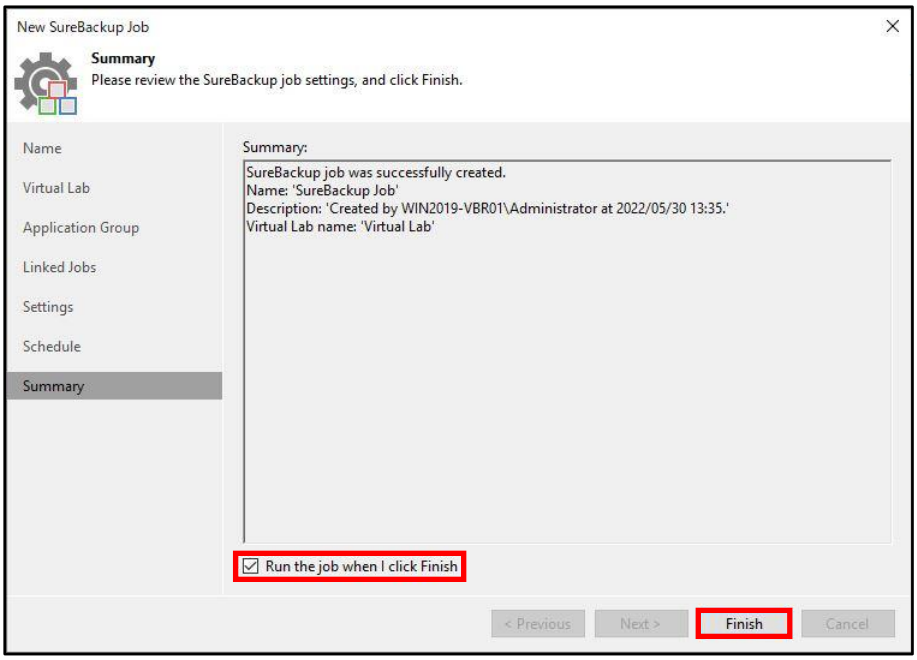
7. [Next >]をクリックします。



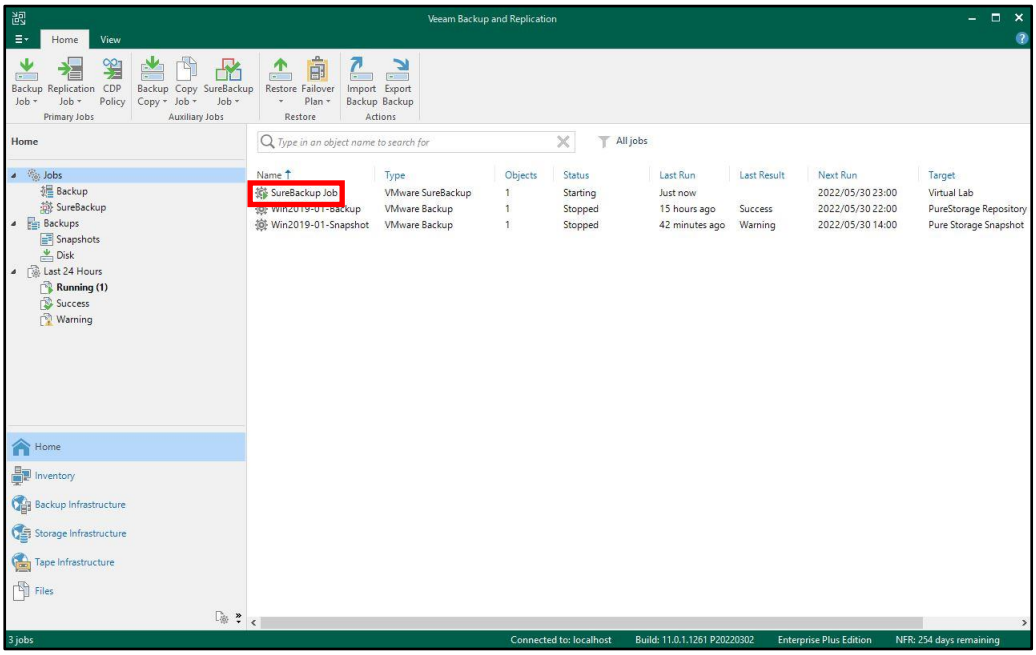
8. [Run the job automatically]にチェック後、Daily at this time:に[23:30]と入力して[Apply]をクリックします。



9. 本書ではジョブ作成後にジョブを即時実行しますので、[Run the job when I click Finish]にチェックを入れて[Finish]をクリックします。

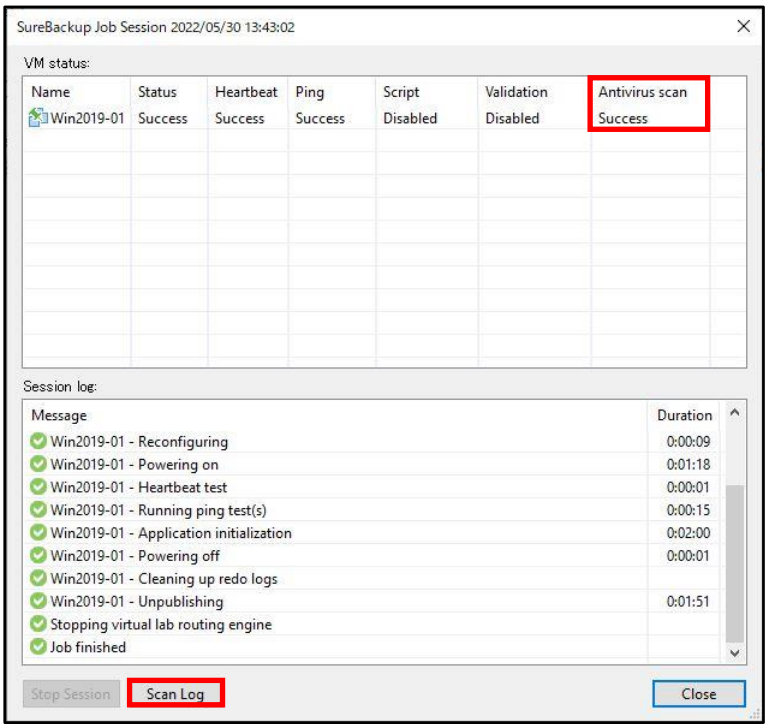


10. SureBackup ジョブ名をダブルクリックします。



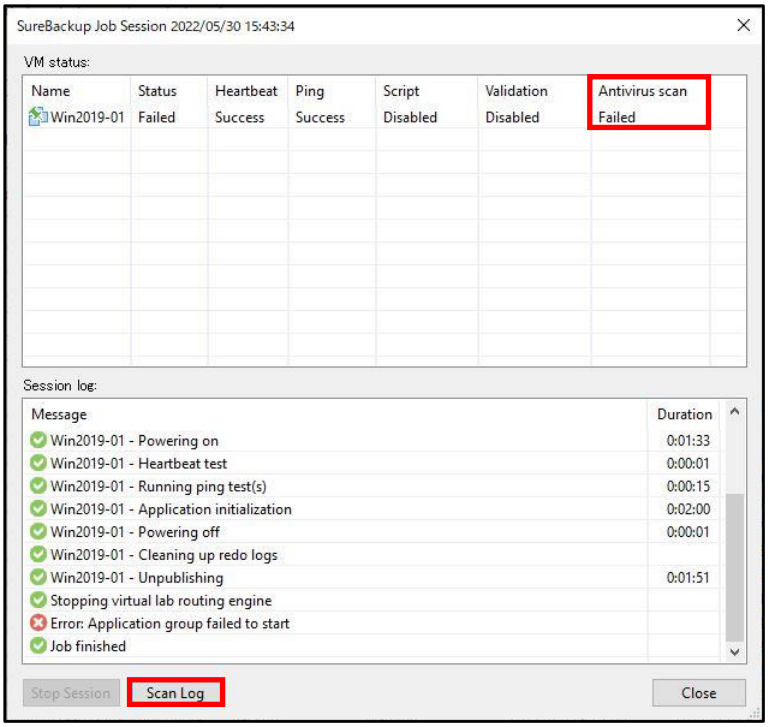
11. ジョブのステータスが表示されます。 Antivirus scan でウィルスやマルウエアが検出されなかった場合は[Success]、検出された場合は[Failed]と表示されます。 ※[Scan Log]をクリックするとスキャン結果が表示されます。

・ウィルスやマルウエアが検出されなかった場合



・ウィルスやマルウエアが検出されなかった場合（参考：Scan Log 結果）

・ウィルスやマルウエアが検出された場合
注）本書では、テストファイルを使用して確認しています。



・ウィルスやマルウエアが検出された場合（参考：Scan Log 結果）

以上で SureBackup ジョブの作成と実行は完了です。

6.5. Secure Restore

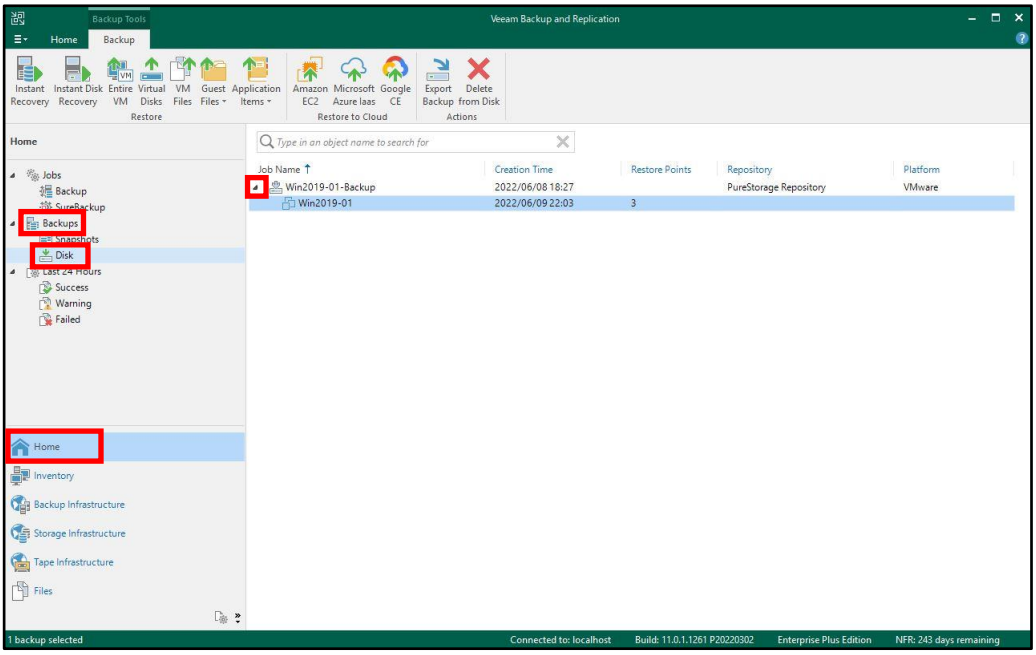
Secure Restore を使用すると、バックアップがウィルスやマルウエアに感染していないことを検証することによって、最初の感染や再感染の恐れなくデータを安全にリストアできます。

Secure Restore は、次のリストア操作で利用できます。

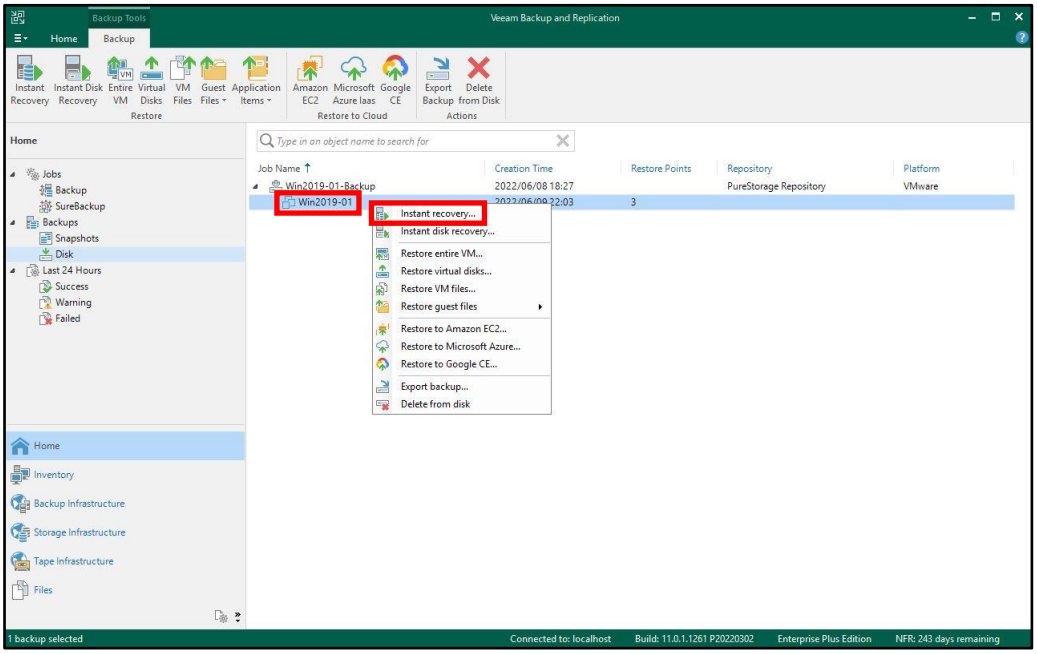
- インスタントリカバリ
- VM 全体のリストア
- 仮想ディスクのリストア
- Microsoft Azure へのリストア
- Amazon EC2 へのリストア
- Google Cloud へのリストア
- ディスクのエクスポート

本書では、インスタントリカバリ時に Malware scan を実行しバックアップがウィルスやマルウエアに感染していないことを確認する手順について説明します。

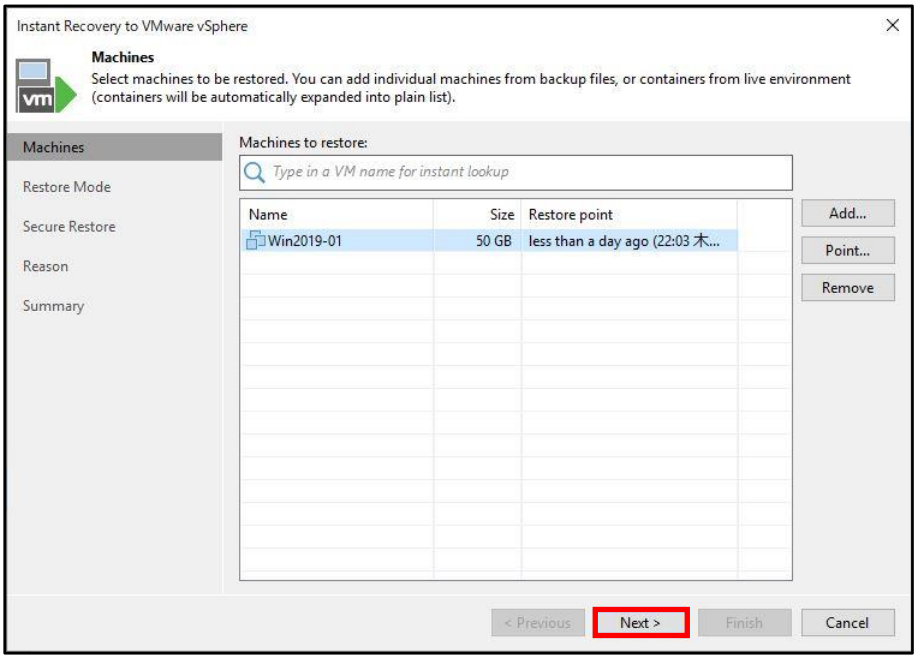
1. Veeam Backup & Replication Console の[HOME]-[Backups]-[Disk]-[▶]をクリックします。



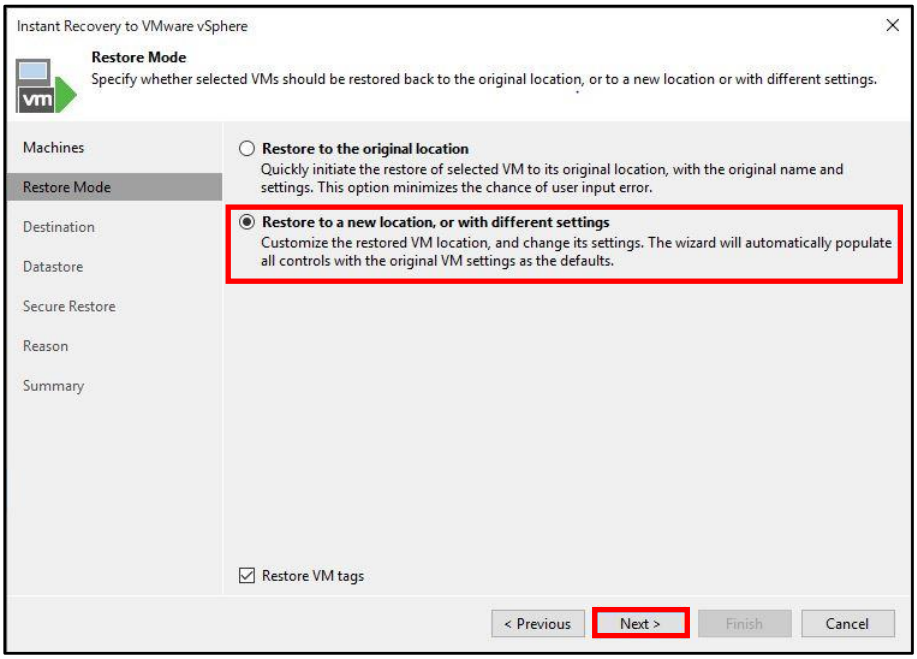
2. リストアする仮想マシンを右クリックして、[Instant recovery...]をクリックします。



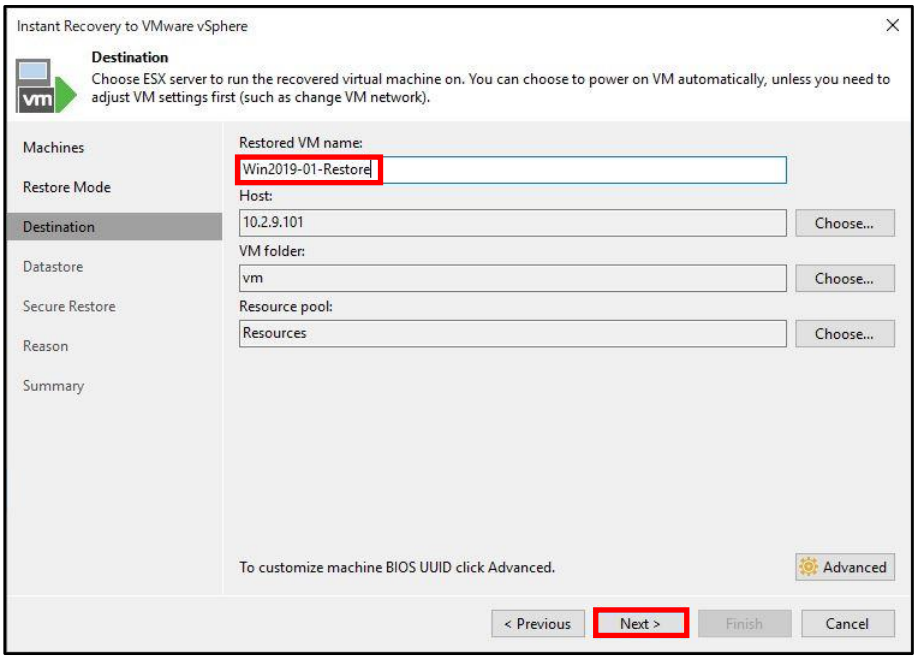
3. 本書では最新のリストアポイントを使用しますので、そのまま[Next >]をクリックします。
※過去のリストアポイントを指定する場合は、バックアップファイルを選択して[Point...]をクリックします。



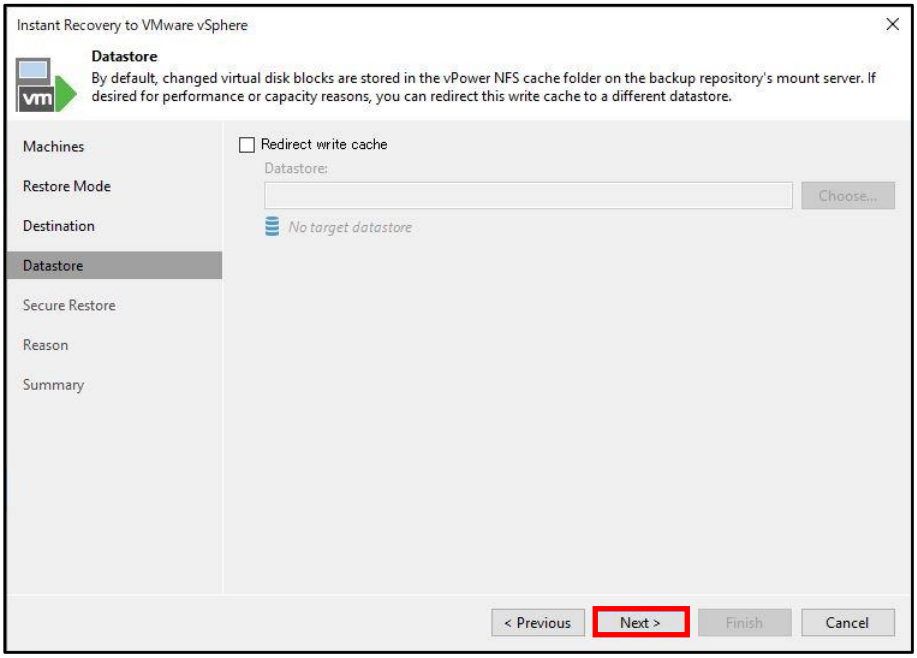
4. [Restore to a new location, or with different settings]にチェックを入れて、[Next >]をクリックします。



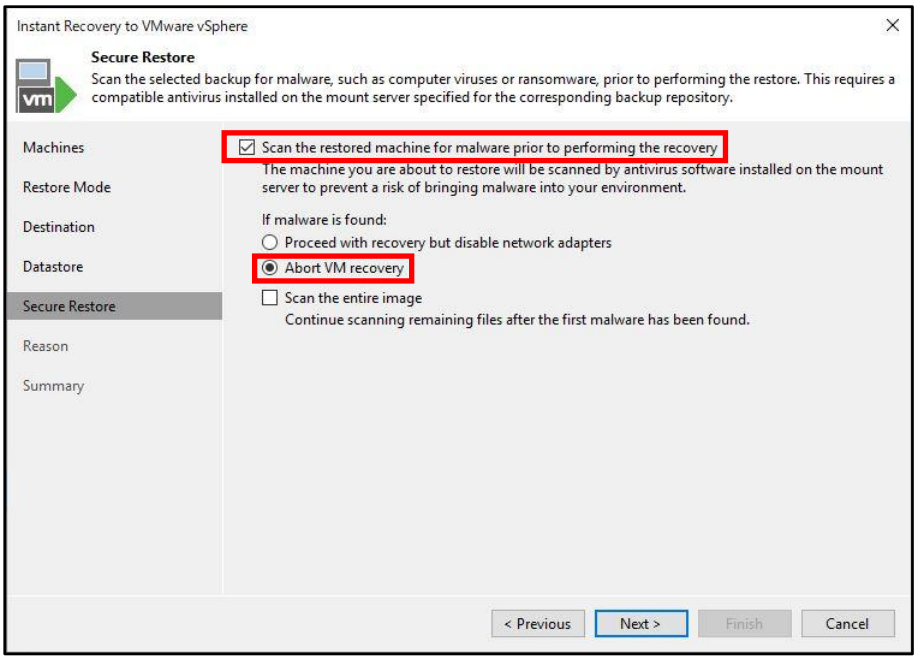
5. 任意のリストアする仮想マシン名を入力して、[Next >]をクリックします。
※本書では、デフォルトの ESXi ホストにリストアしています。



6. [Next >]をクリックします。



7. Malware scan を実行しますので、[Scan machine for virus threats prior performing recovery] にチェックして、[Abort VM recovery]を選択します。



参考：

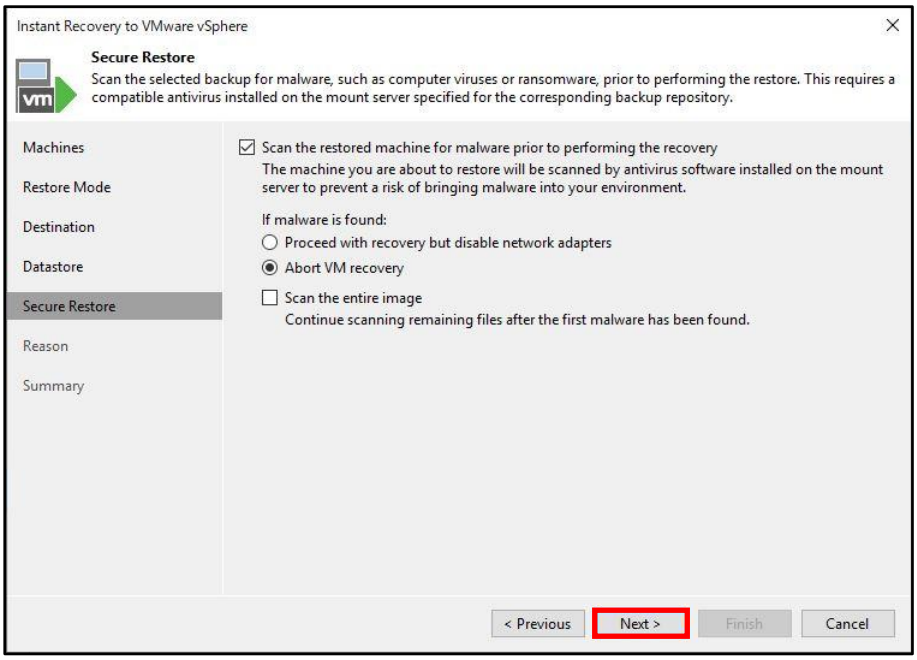
If malware is found:

・Proceed to recovery but disable VM network adapters：
ウィルスやマルウエアが検出された場合、ネットワークアダプタ（NIC）を無効にした仮想マシンをリストアします。

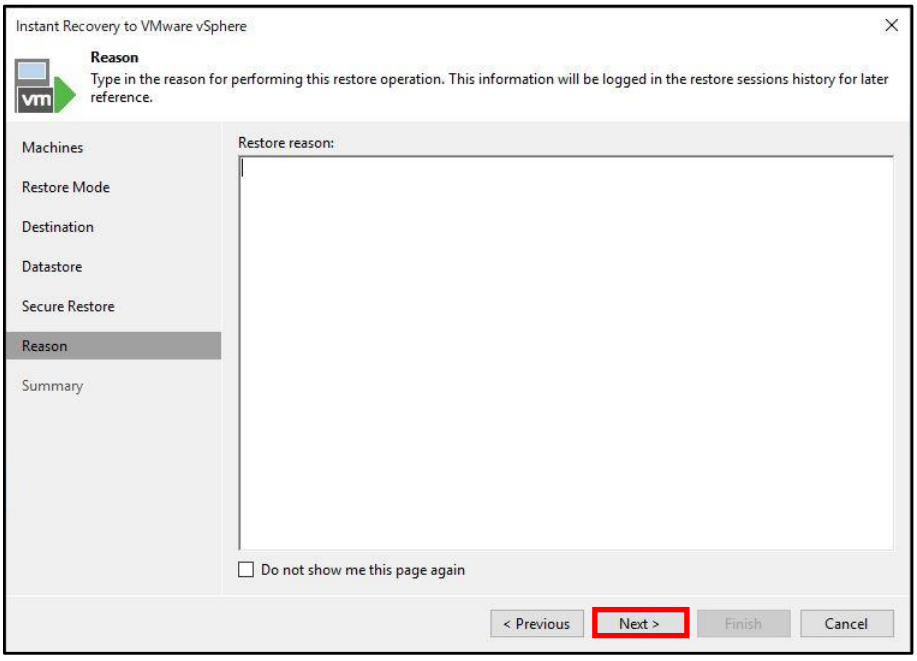
・Abort VM recovery：
ウィルスやマルウエアが検出された場合、リストアセッションをキャンセルします。

・Scan entire VM for virus threats：
最初のマルウエアが検出された後も Malware scan を継続します。

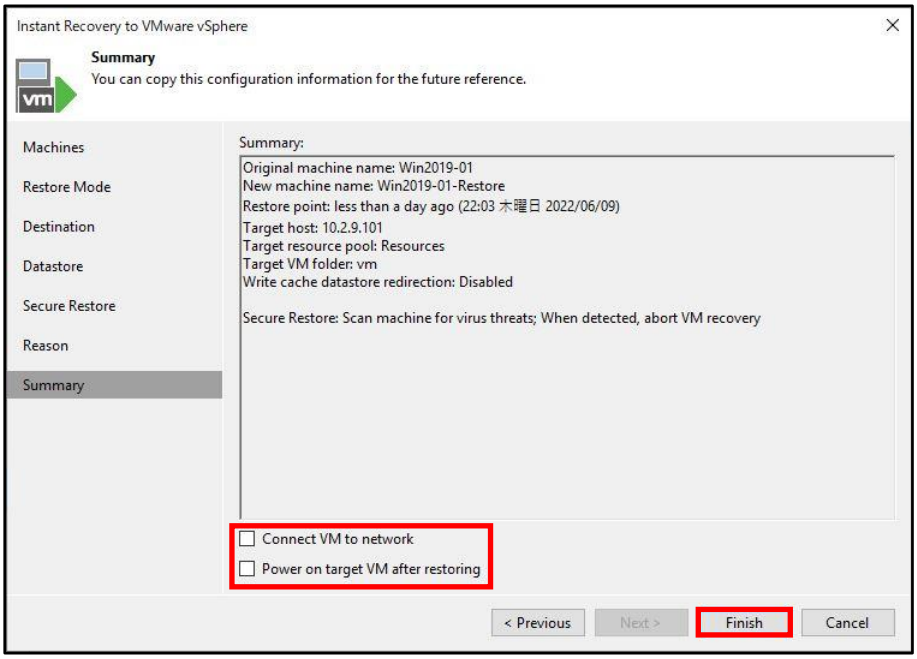
8. [Next >]をクリックします。



9. Reason でコメントを入力できますが、そのまま[Next >]をクリックします。

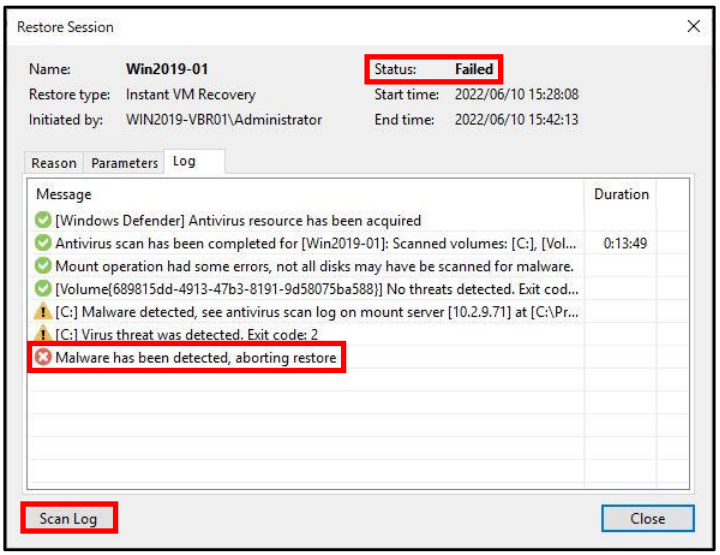


10. 本書ではバックアップがウィルスやマルウエアに感染していないことだけを確認するため、仮想マシンの起動やネットワークは接続しませんので、[Connect VM to network]、[Power on target VMs after restoring]のチェックを外して [Finish]をクリックします。
ジョブ作成後にジョブが即時実行されます。



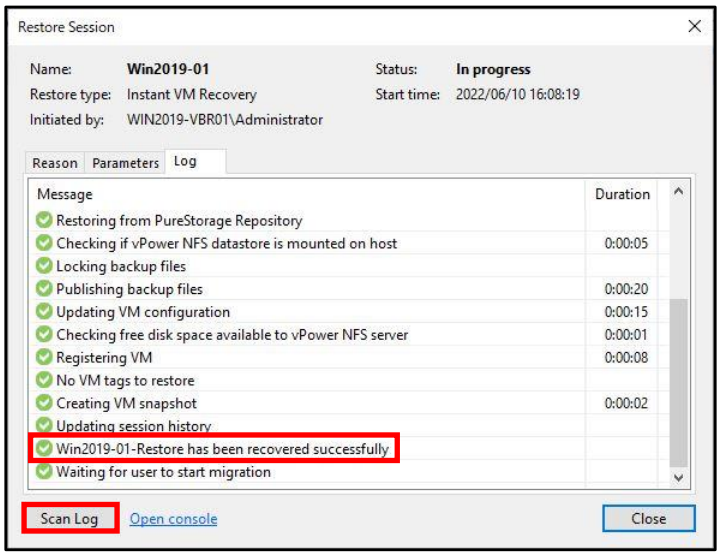
11. ジョブのステータスが表示されます。 Antivirus scan でウィルスやマルウエアが検出された場合は[Malware has been detected, aborting restore]と表示されリストアが終了します。
Antivirus scan でウィルスやマルウエアが検出された場合は、1～10 の手順を繰り返しリストアポイントを遡ることで安全なバックアップを確認することができます。
※[Scan Log]をクリックするとスキャン結果が表示されます。

・ウィルスやマルウエアが検出された場合
注）本書では、テストファイルを使用して確認しています。



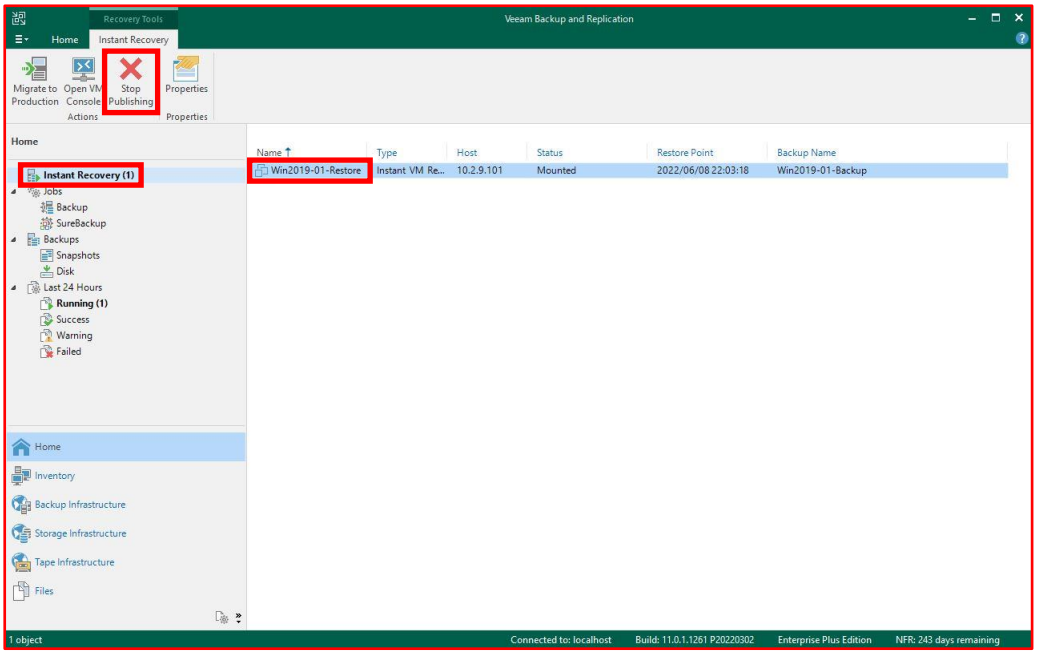
・ウィルスやマルウエアが検出された場合（参考：Scan Log 結果）

・ウィルスやマルウエアが検出されなった場合

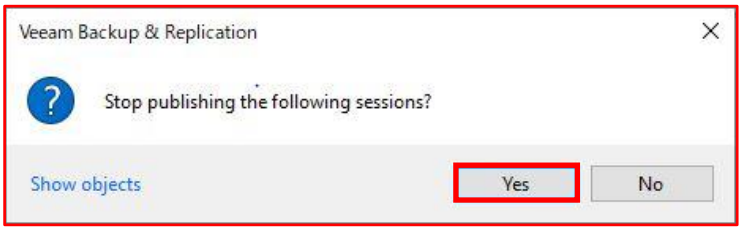


・ウィルスやマルウエアが検出されなった場合（参考：Scan Log 結果）

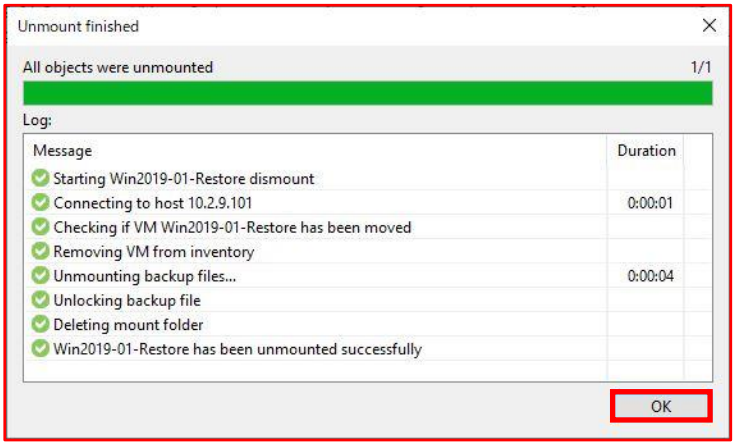
12. 作成したジョブ名を右クリックして、[Stop publishing]を選択します。
※本書では、[Stop publishing]を選択しましたが、本番ストレージに移行する場合は[Migrate to Production]や[ストレージ vMotion]などで移行してください。



13. [Yes]を選択します。



14. [OK]をクリックします。



以上で Secure Restore は完了です。

6.6. SafeMode を利用したストレージスナップショットのリカバリ手順

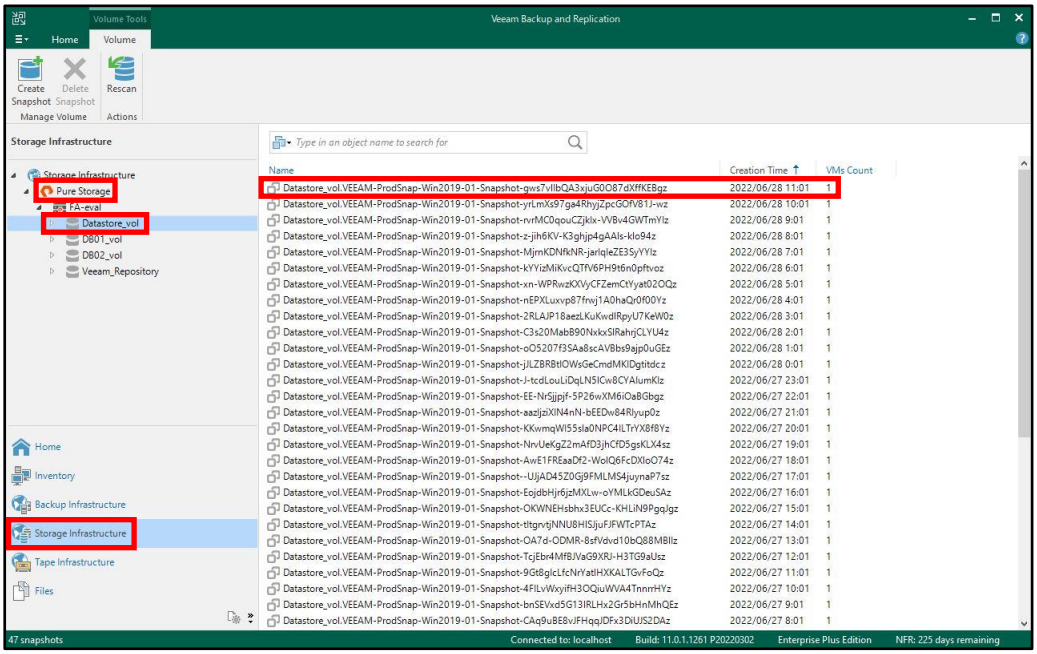
SafeMode は、FlashArray に組み込まれたデータ保護機能です。 スナップショットが提供する不変性保護を拡張し、SafeMode によって Eradicate 操作(手動による各種データの完全削除操作)を無効化した期間内であれば仮に FlashArray の管理者権限を奪われてしまったとしても、データが意図的に削除されてしまうことを防ぎ、リカバリすることが可能です。

SafeMode:

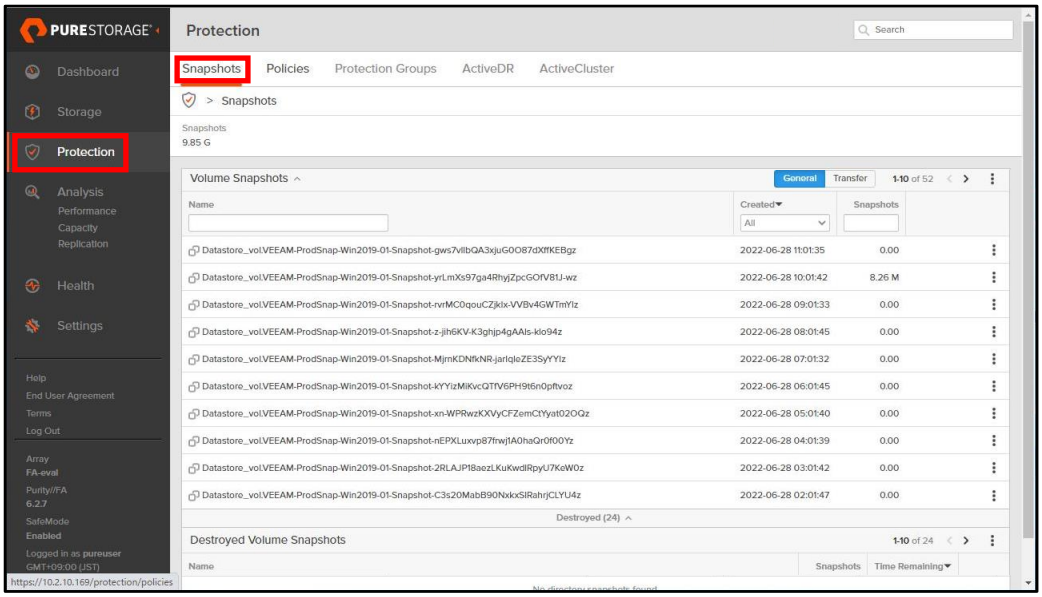
- Destroyed からオブジェクトを手動で削除(完全削除)する機能を無効にします。
- 24 時間から 30 日間までの間で各種データ(Volume や Snapshot)の Eradicate 操作不可期間(手動による完全削除操作を無効化する期間)を設定可能です。
- Protection Groups のスケジュール設定によって定義された Snapshot 保持期間を短縮する操作や Snapshot 取得サイクルの間隔を延ばす操作を無効にします。

本書では、Pure Storage の管理者アカウントでストレージスナップショットを削除し Pure Storage の GUI からリカバリする手順について説明します。

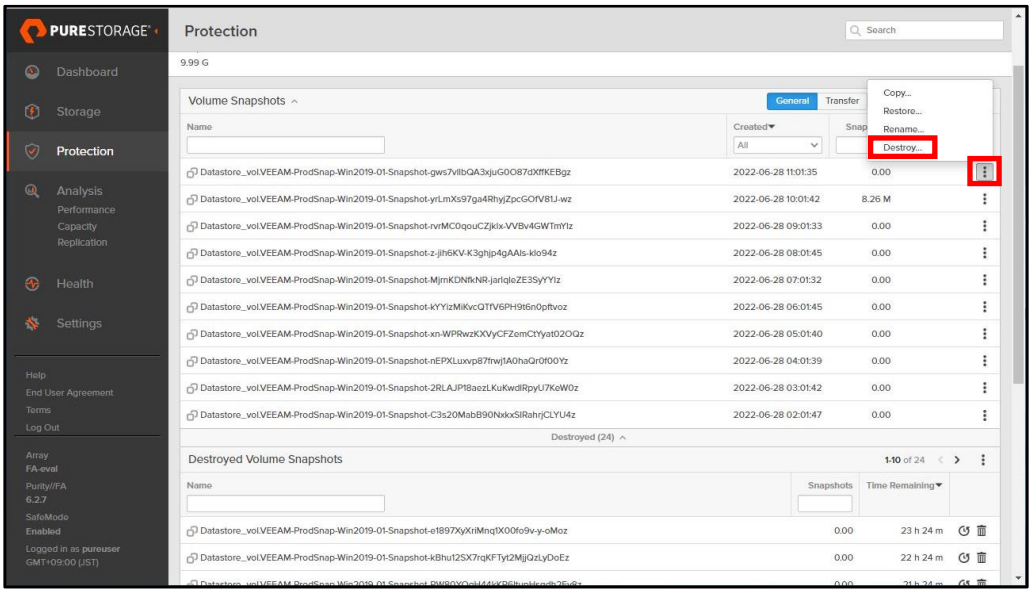
1. Veeam Backup & Replication Console の[Storage Infrastructure]- [Pure Storage]からスナップショットがあるボリュームをクリックして、最新のスナップショットを確認します。



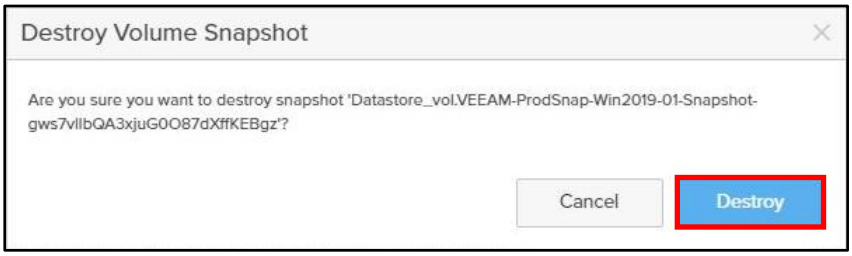
2. Pure Storage の GUI から[Protection]-[Snapshots]をクリックします。



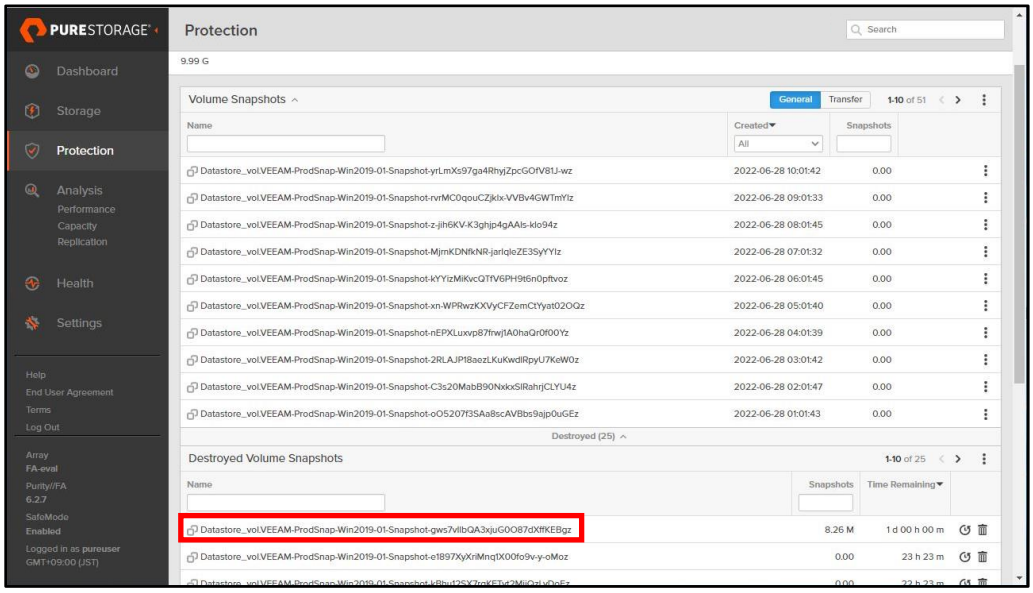
3. 1.で確認したストレージスナップショットのケバブメニューから[Destroy...]をクリックします。



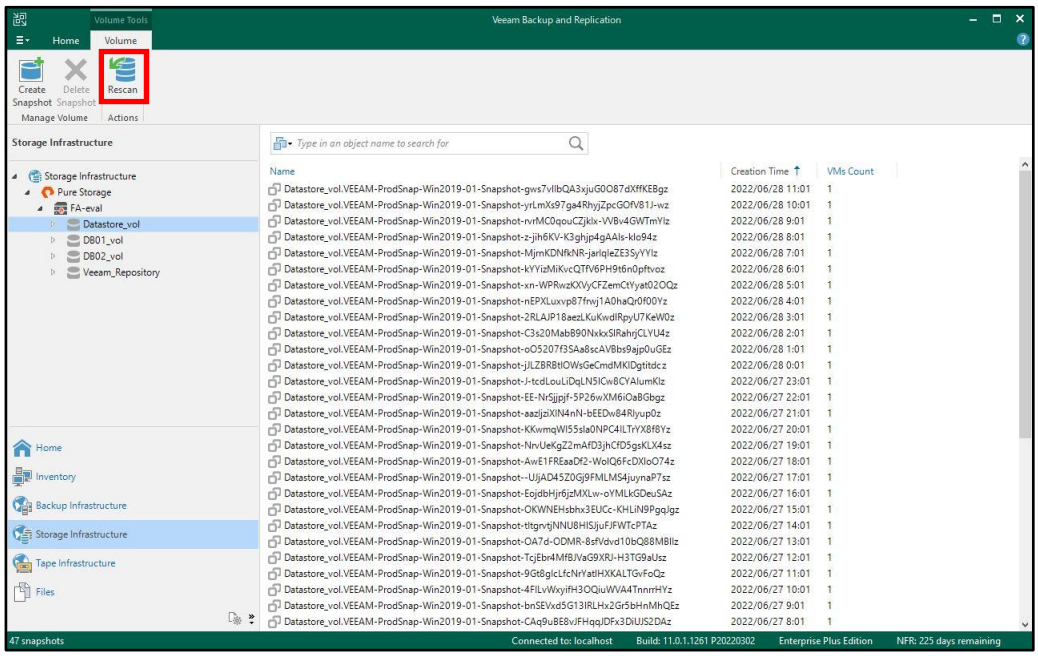
4. [Destroy]をクリックします。



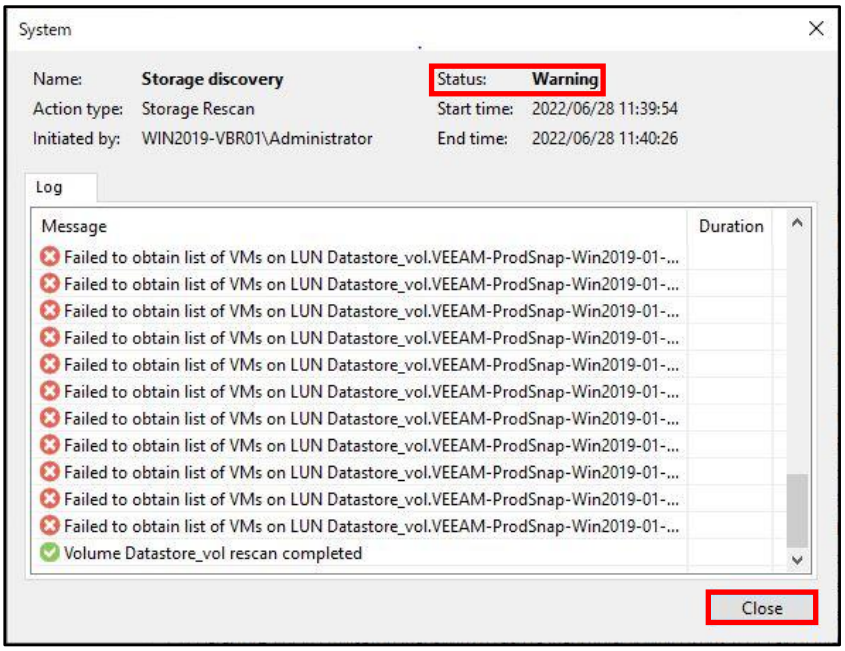
5. Destroyed に Destroy したストレージスナップショットが表示されていることを確認します。



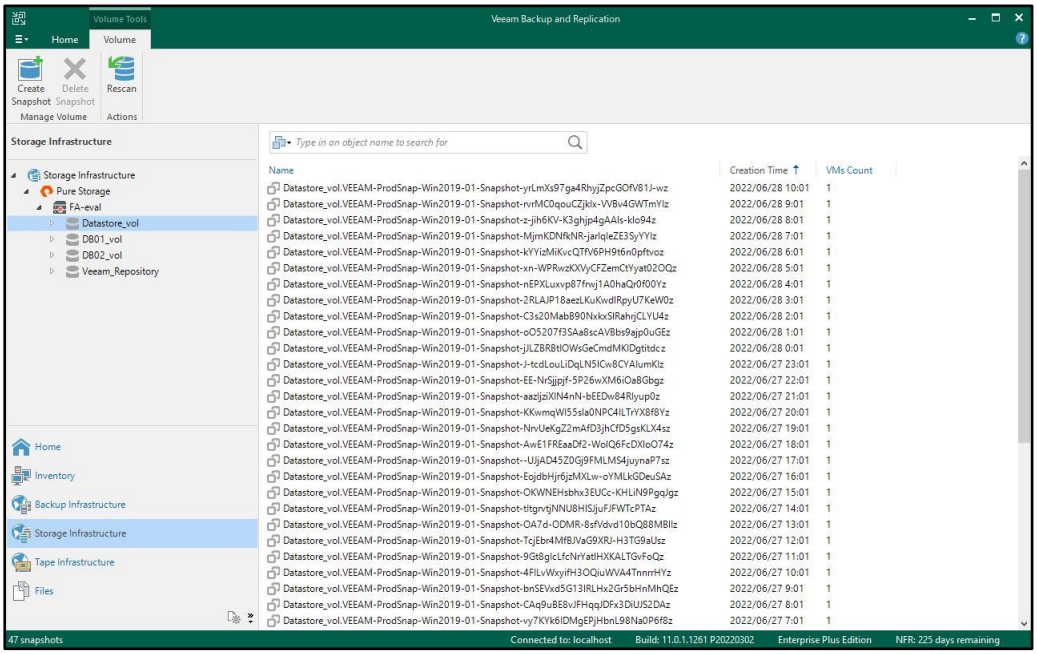
6. Veeam Backup & Replication Console に戻って、[Rescan]をクリックします。



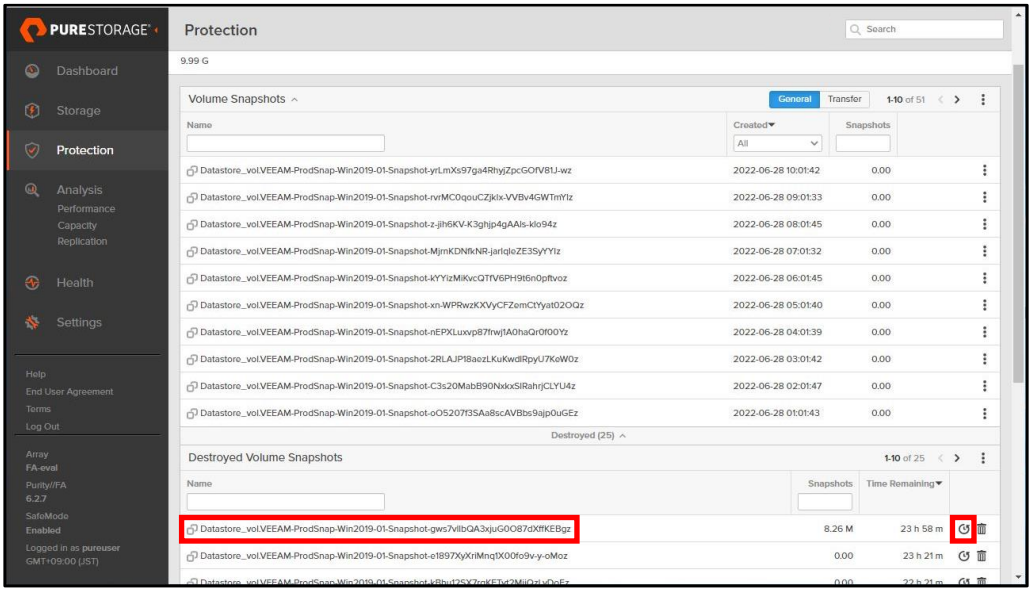
7. Status が Warning になりますが問題ありませんので、[Close]をクリックします。



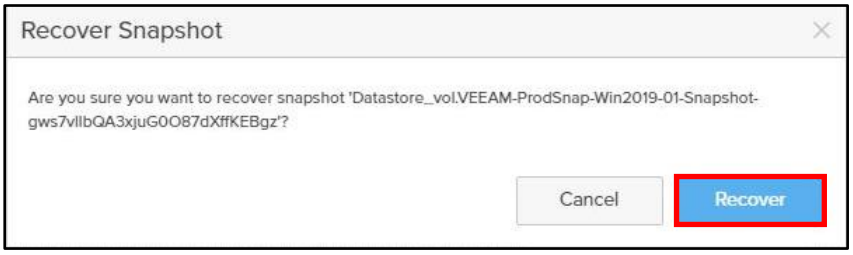
8. Destroy したストレージスナップショットが表示されていないことを確認します。



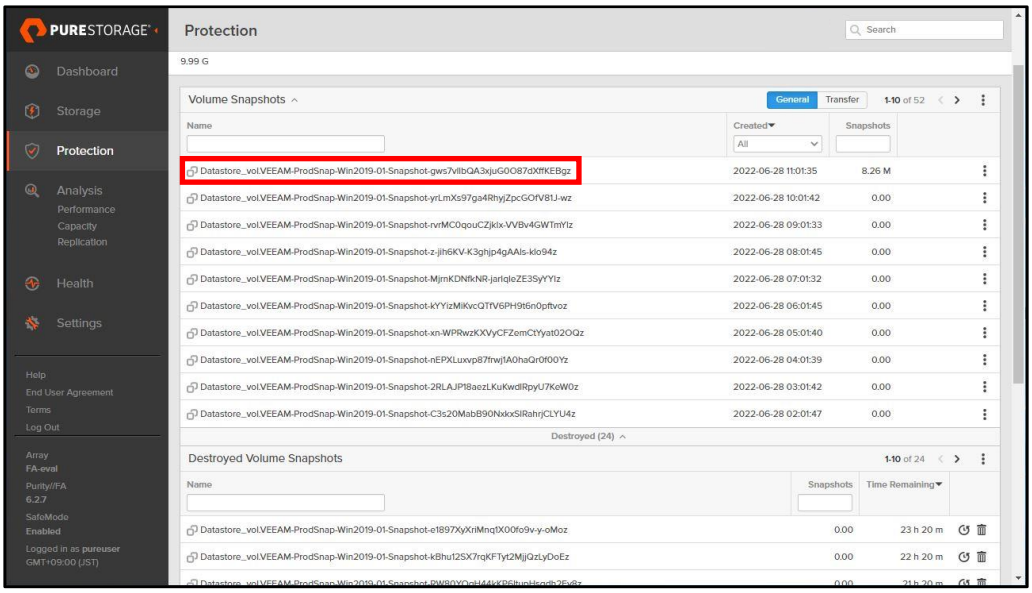
9. Destroy したストレージスナップショットをリカバリしますので Pure Storage の GUI に戻って、Destroyed にあるストレージスナップショットのタイマーアイコンをクリックします。



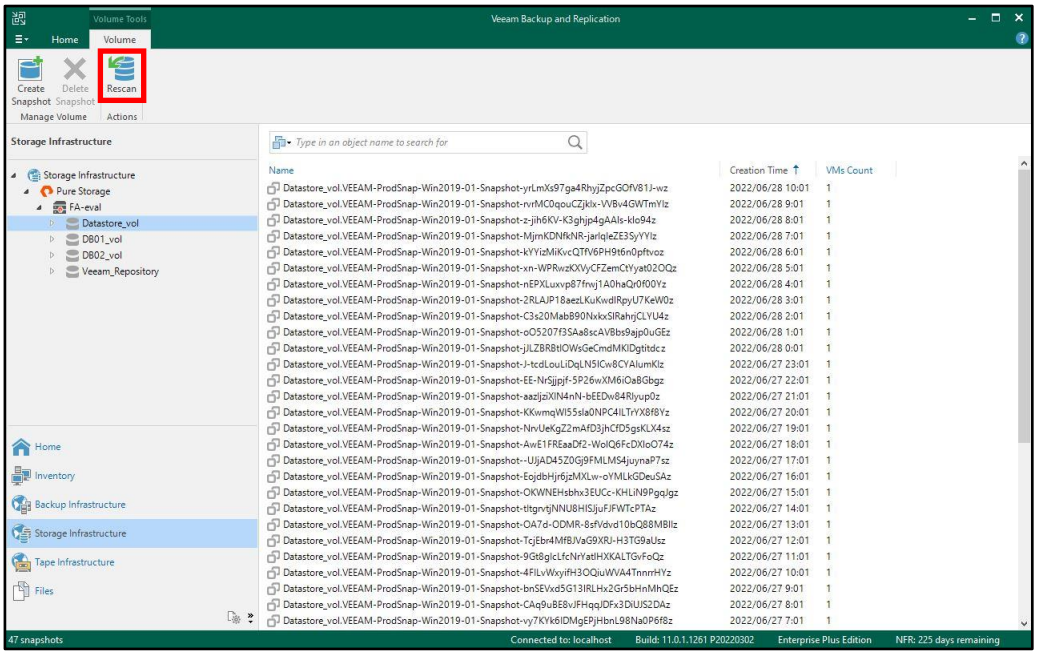
10. [Recover]をクリックします。



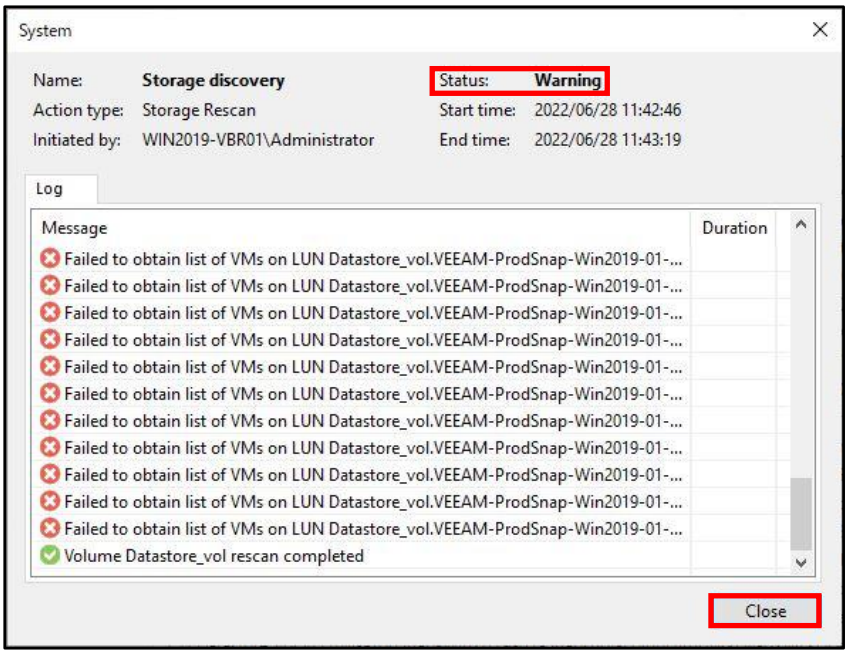
11. リカバリされたスナップショットを確認します。



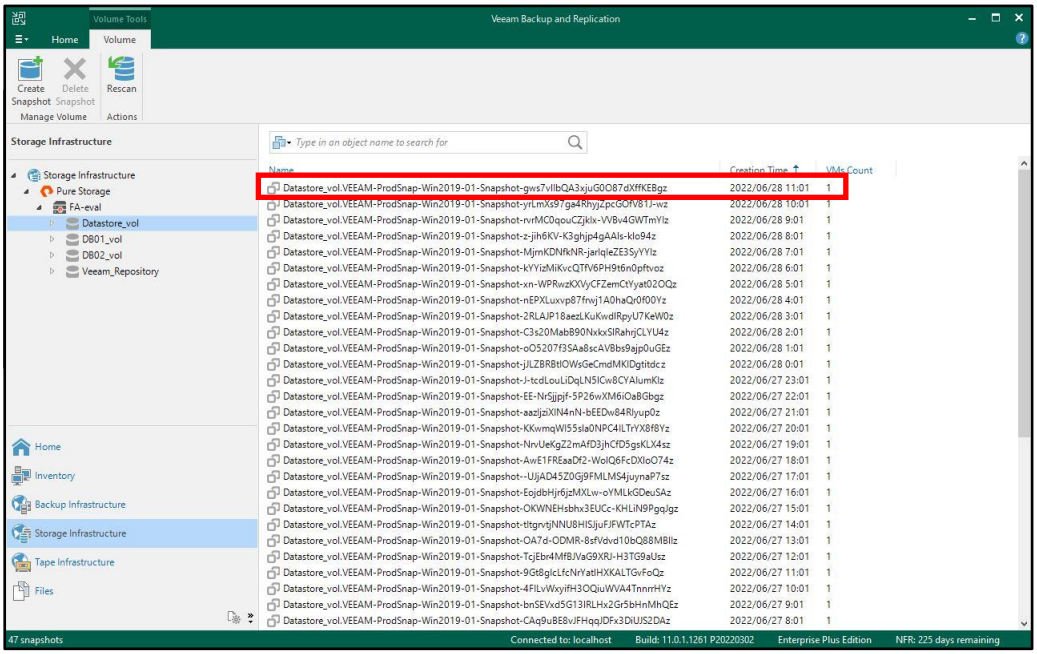
12. Veeam Backup & Replication Console に戻って、[Rescan]をクリックします。



13. Status が Warning になりますが問題ありませんので、[Close]をクリックします。



14. スナップショットがリカバリされたことを確認します。



以上で SafeMode を利用したストレージスナップショットのリカバリ手順は完了です。

7. まとめ

Veeam Backup & Replication と Pure Storage FlashArray の連携機能を使用することで、バックアップ時の VM Stun やスナップショット取得時の負荷を軽減するとともにスナップショットオーケストレーションと組み合わせて RPO をさらに向上させることが可能です。

また、ランサムウエア対策として強化 Linux リポジトリによる書き換え不能なバックアップ、Pure Storage の SafeMode を利用することでバックアップやストレージスナップショットの削除、変更、暗号化ができないため、ランサムウエアの攻撃から保護することが可能です。

SureBackup、Secure Restore は、ウィルスやマルウエアの検知や安全なリストアを行うことができます。

導入をご検討の際には、ぜひ弊社にお声がけください。

参考文献

- Veeam Backup & Replication 11 User Guide for VMware vSphere
  https://helpcenter.veeam.com/docs/backup/vsphere/overview.html?ver=110
- Linux Server
  https://helpcenter.veeam.com/docs/backup/vsphere/linux_server.html?ver=110
- Hardened Repository
  https://helpcenter.veeam.com/docs/backup/vsphere/hardened_repository.html?ver=110
- SureBackup
  https://helpcenter.veeam.com/docs/backup/vsphere/surebackup_recovery_verification.html?ver=110
- Secure Restore
  https://helpcenter.veeam.com/docs/backup/vsphere/av_scan_about.html?ver=110