

Backup Migration and Consolidation

Technology Concepts and Business Considerations

Abstract

This white paper provides an overview of the considerations, benefits, and timescales that are typically considered when migrating from one backup software provider to another backup software provider. It attempts to provide guidance on the approach, the steps expected, and the effort required during such an exercise. The paper also highlights some of the key benefits and advantages that can be gained with proper planning of the migration scope, design, execution, and handover phases.

March 2009

Copyright © 2009 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Part Number h6132

Table of Contents

Executive summary	4
Introduction	4
Audience	4
NetWorker overview	5
EMC backup and recovery.....	5
Backup software migration.....	6
Why are you migrating	6
Common questions	7
Planning	13
Delivery	13
Execution and timescales	14
Conclusion	15

Executive summary

The use and choice of backup software from a specific provider are often mandated and typically the result of some historical event. This may have been a comprehensive review that took into account all requirements and available options before concluding on a single backup provider. However in many cases, this was not the case and the backup provider was the result of a legacy situation, policy, or reasoning that may no longer be valid. In many cases, current IT and business conditions may have shifted significantly enough to render a current backup solution inadequate. It is therefore valid to question the current backup supplier and the infrastructure and technology that it uses, and determine if the choice of these elements meets the current business requirements for data protection and service recovery.

There are many backup products in the marketplace and each uses a variety of different technologies and approaches. It is possible that you are not relying on a single backup provider or common technology but have “collected” a number of different backup solutions through acquisition and consolidation. This often leads to a more complex and inefficient backup and recovery service that is difficult and costly to maintain.

The decision to move to a new backup vendor may be a result of service level achievement difficulties, business conditions, or a formal consolidation program. No matter the case, the move to a single, consolidated backup environment provides an opportunity to simplify, consolidate, and manage the backup and recovery service more effectively and efficiently. It also provides opportunities to benefit from the latest technologies, and simplified and consistent service levels, ensuring sufficient growth, management and reporting capabilities for the future. Moving to a consolidated backup environment also provides the opportunity to reduce employee costs by enabling administration from a common technology rather than from many different technologies. This improves the responsiveness and quality of service provided by the backup operations.

For clarification the term migration used in this paper refers to migrating the backup environment and not the migration of legacy backup data to the new backup application.

Introduction

This white paper provides an overview of the considerations, benefits, and timescales that are typical when migrating from one backup software provider to another backup software provider. It provides guidance on the approach, the expected steps, and the effort required during such an exercise. The paper also highlights some of the key benefits and advantages to be gained that should be considered during the migration scope and design phases.

By providing the reader with a background on the steps commonly needed to be successful in a migration between backup software providers, this paper helps the reader understand and more easily evaluate the scope and proposal of any migration being considered. With insight into the approach needed to complete a migration, effort and disruption are minimized and the benefits can be fully realized.

Audience

This paper has been written for technical managers and decision-makers, procurement specialists, architecture consultants, and senior administrators who wish to gain an appreciation of the benefits, effort, timescale, and approaches that are likely to be involved when moving from one backup provider to another.

The paper does not cover the technical differences in individual products, best practices, or recommendations for the design or implementation.

NetWorker overview

EMC® NetWorker® enterprise backup and recovery software centralizes, automates, and accelerates data backup and recovery across IT environments. Boasting record-breaking performance and flexibility, NetWorker protects critical business data in a fast, secure, and easy-to-manage way. NetWorker features include the following:

- Centralized backup and recovery across SANs, NAS, and direct-attached storage
- Advanced backup and integration with replication technologies to provide higher degrees of protection and recoverability
- Heterogeneous platform support to protect UNIX, Windows, Linux, NetWare, OpenVMS, Macintosh, Hyper-V, and VMware operating systems with a common interface
- Comprehensive application coverage for Oracle; Microsoft SQL Server, SharePoint, Exchange, and Data Protection Manager; IBM DB2 UDB; Informix; Lotus Notes/Domino; SAP; Sybase, EMC Documentum® and MEDITECH
- Leading capabilities for virtual environment protection, including VMware and Hyper-V, to ensure you get the most value from virtualization, including integration with EMC Avamar® for high performance, source-based deduplication
- Off-host backup to eliminate the impact of data protection from production servers
- Global data deduplication – reducing data at the source to speed backups, reduce bandwidth and resource consumption, and lower overall backup storage requirements
- Advanced backup-to-disk, staging and cloning, embedded VTL capabilities, target-based deduplication support, CDP, replication, and snapshot management to meet any RTO and RPO requirement
- State-of-the-art, 256-bit AES encryption and enhanced user authentication to meet increasing security requirements

EMC backup and recovery

EMC offers the industry's broadest set of hardware, software, and services that strengthen, streamline, and simplify your data protection operations. With the best of traditional and next generation backup technologies, including backup-to-tape and disk, source and target-based deduplication, virtualization integration, snapshot management, continuous data protection (CDP), and state-of-the-art analytic tools to predict, troubleshoot, and optimize the backup environment, EMC helps you protect and recover data effectively with the scalability and flexibility your organization requires. Moving to next generation backup and recovery enables your organization to:

- Ensure investment protection
- Manage backup software license costs
- Control backup software maintenance costs
- Reduce migration and training costs

EMC leverages the industry's broadest portfolio of backup and archiving solutions to ensure you get the right solution for your backup challenges. Remove risk by drawing on EMC's deep expertise built on more than 15 years of backup and recovery experience. These solutions include the following.

EMC Disk Library family

- Industry-leading VTL, now with the power of policy-based data deduplication
- Works with existing backup applications and tape infrastructure
- Flexible solutions from small to large environments
- High performance, direct tape creation, and high availability architecture

EMC Avamar

- Industry-leading backup and recovery solution with global source-based deduplication
- Deduplicates at the beginning of and throughout the backup process
- Recover in one step (no more incrementals!)

EMC Data Protection Advisor

- Industry-leading data protection management solution, providing active management, monitoring, and reporting
- Support for multiple backup applications
- File system (NAS), database, and virtualization options

EMC RecoverPoint family

- Industry-leading continuous data protection (CDP) and continuous remote replication (CRR) with SAN and array integration
- Replication options for local and remote recovery

Backup software migration

Why are you migrating

There are many reasons why a migration from one backup solution to another makes sense. It is likely you have already identified a driver for considering a migration that is key to your business and a result of problems that you are facing today with your current backup and recovery environment. A migration from one product to another provides a number of significant benefits and options that should be understood and considered. The migration process presents a unique opportunity to evaluate, streamline, and modernize operation procedures and management of the environment.

Some common reasons for migrating are listed next together with a brief explanation and some typical examples. Depending on your situation some of these may not be relevant based on your unique environment or situation; however, it is important to consider all the benefits available to ensure that the effort in migrating from one product to another provides the maximum value to you and your business. For example, this may be an ideal time to solve an offsite data problem, improve your SLAs and compliance reporting, or get rid of unreliable and costly legacy equipment.

There are many other areas that could also be considered, such as consolidating different standards and policies or more dramatic changes such as data classification or refreshing the infrastructure in some way. Ideally, the migration from one backup product to another should not be justified by a single reason; rather a migration should be rationalized when *multiple reasons, benefits, and drivers are identified*.

- **New features / technologies**

Backup products and infrastructure differ and evolve. There is likely to be new and different technologies that allow you to back up and recover faster and easier with more flexibility. For example:

- Deduplication and snapshot technologies provide greater performance and protection.
- Virtualization of different environments creates different requirements, SLAs, and infrastructure needs.
- Archiving of static information requires different techniques and technologies and can have significant impact on data protection.

- **Technology limitations**

Operating systems, applications, and hardware often are added to the IT environment without much regard to the backup infrastructure. This often presents support and functionality issues, which can be solved only by creating custom solutions or costly upgrades. For example:

- The latest dual-core, 64-bit CPUs often require software and technologies for backup and recovery.
- The latest Microsoft applications use a different backup interface and need updated software and infrastructure to enable simple and fully supported backup and recovery.

- **Maintenance cost**

Once you have software that meets a business need, you have few options to negotiate or change the terms of support costs. These costs often increase with little notice or reason or service may decline, resulting in poor value for money from your precious IT budget.

- Do you have legacy or older software that is now much more expensive to support?
- Is the service provided by your current supplier meeting your business needs and SLAs?

- **Scale limitations**

- Is your backup server now processing more clients, applications, backup sessions, and devices than it was designed for?
- Do you have to remove tapes from your tape library to ensure that enough capacity is available?

These are typical limitations that prevent you from scaling your existing environment, leading to ad hoc solutions and expensive upgrades and disruption. The backup catalog is now so large and takes too long to update, too long to back up, and too difficult to get reports. The environment needs constant attention just to keep it going. These are typical of the problems that can be eased or solved by redesigned and improved processes and reporting.

- **Service support**

Solution technical support often is geared to what the supplier wants to supply and seldom matches the support requirements of the business.

- Do you have multiple contacts and companies providing your support?
- Do they meet your needs and SLAs?
- Are they providing the service for which you paid?

Look at the response and call closure times from you solution providers. Ask about designated or onsite engineers or regular site visits and training packages. Can they ensure your success?

- **Data center consolidation / moves / acquisitions**

Acquisitions and departmental / regional consolidations often create pockets of infrastructure. Different products and disparate solutions are difficult and costly to support and maintain. Look at sharing and centralizing infrastructure and support to make efficient use of your resources, freeing up capacity and skills.

- Does the technology allow for infrastructure such as remote offices to be moved to a central location, eliminating costly and difficult support situations?
- Does the technology permit centralized monitoring and protection of remote assets?

Common questions

There are a number of questions that arise as you look to plan a migration from one backup provider to another. Most of the questions require definition, investigation, and exploration before they can be answered and a decision can be made. Some of the questions will be specific to your environment; however, there are common questions that should be asked during *any* migration. The following are some common questions with brief explanations and some hints and tips to how they can be answered to control issues and reduce concerns.

- **What will it cost?**

Migration costs can be divided into three related areas: planning costs, infrastructure costs, and deployment costs. The costs for each will depend on the skills available and the size, complexity, and knowledge of the current environment. As every customer and migration is unique it is impossible to provide estimates for costs without further investigation and details.

When assessing costs for migration it is important to consider the immediate and the long-term benefits. The costs to keep the existing environment should also be considered as these are often subject to change. Additional effort to maintain and improve a legacy environment is likely to be needed, which will incur further cost and effort and may not meet or satisfy your business needs. It should also be recognized that during the migration the personnel will manage both the legacy application and the new application until the migration is complete.

- **Planning costs**

Time is money. The longer it takes to gather data and understand the environment, the longer and more costly the planning stage will become. It is tempting to limit the time gathering data and planning the migration; however, the risk of improper planning is that you encounter problems during the deployment phase, where unexpected events will produce delays and risks. Here are some tips for controlling the overall costs and minimizing effort and risk during the planning phase.

- Consider spending more time and investing up front to get good information. This will make the scope, design, and decision process easier and will pay dividends beyond the migration. An assessment or the use of analysis tools can provide accurate data very quickly and will reap benefits during and after the migration.
- Be prepared to use existing modules or new techniques to secure systems and services. Focus on the requirement, not the existing process.
- Be prepared to change or adapt processes. Focus on the requirement, not the existing process.
- Complexity leads to error and costs. Keep the processes and deployment configurations to a minimum.
- Consider limiting the scope to the core or a subset of the environment. Focus on the more complex areas as simpler sites can be migrated at a later stage and can be done with your own staff or with less resource.

The types of areas that typically increase costs are:

- Limiting the amount of time that is devoted to analysis and design of the solution. This impacts the ability of the solution to meet customer expectations, reduce escalations, and make the migration smoother.
- Lack of detail and knowledge of current environment and the performance or SLAs that it is currently providing or attempting to provide
- Scripts or customization of existing software to perform tasks that are unique to the site and that are difficult to support and manage
- Complex and multi-step backup processes – especially when they involve custom scripts (synchronize, snapshot, mount, backup, etc.)
- Multiple sites and buildings, especially when these are large in number or dispersed by hundreds of miles with different communications links and local skills
- Lack of knowledgeable people or access to the right people
- Scope changes or lack of clear decision-making. These cause work to be repeated or changed, which causes delay and increases costs.

- **Deployment costs**

The deployment costs can also be divided into three areas: complexity of the design, resources available to manage both the legacy environment with the new environment, and the time permitted to deploy. It is perfectly acceptable to want to control and limit the amount of time that is spent migrating from one software product and environment to another. External influences such as contract renewals, new services, and other business priorities often need to be considered. However

the amount of time and effort to complete a given design is essentially fixed. Any restrictions in time will result in increased effort (resources) being required or an incomplete design so this clearly affects the costs of the deployment. Adding more resources does not necessarily decrease the time it takes to perform the project. Changes and or lack of understanding of time-related issues will add risk to the deployment if they are not managed appropriately. Therefore adequate time and budget are needed to ensure a successful migration. Some examples of required resources are listed below with some tips to how these can be mitigated or controlled.

- Having local skills available will help to reduce costs. The lack of skills will increase the cost of resources, especially if these resources are needed during evenings and weekends.
- The use of available resources to provide backfill assistance can be a good way to increase success. It allows local teams to get involved and benefit support and operations teams and aids in the knowledge transfer and handover process.
- If the design can be simplified and become a series of repeatable configuration building blocks, it will make deployment and management far easier. This may require a certain level of flexibility with redesign of the backup environment.
- When implementing an EMC solution, have the proposed design and deployment submitted to EMC's Solutions Validation Center (SVC) for review and approval prior to implementation. This reduces the risk of encountering unsupported environments and infrastructure issues.
- New hardware is likely required and should be embraced as it will make the process far easier and faster (reducing cost). Stay focused on simplicity. Evaluate the risk and effort of reusing hardware versus the speed and costs of purchasing new. Bear in mind that your capacity is likely to increase therefore you should ensure that the hardware is able to meet your current and future needs.
- Plan to deploy and operate the new environment to its strengths. Attempting to get the new software to look and behave in the same way as the previous software will result in increased effort and cost. This is also likely to result in a less optimized and unnecessarily customized environment requiring increased support and expansion efforts.
- Ensure that support staff, operations personnel, and internal customers are prepared for some change and as appropriate, some temporary disruption. Focus on requirements and the benefits of the migration and maintain good communications throughout the process.
- Your legacy data policy can be another significant factor on the time and costs to complete a migration project. Examine the value return of migrating data versus the effort and costs involved to determine if they can be justified. This aspect is dealt with in detail later in this document.

- **Infrastructure costs**

The infrastructure costs are made up of the software licences plus the costs of any infrastructure that is needed to implement and deploy the software.

- **How long will it take?**

The time it takes to complete a migration will be a factor of scope and the skills / resources available. The same points that increase cost are also linked to time. The following points are the most common aspects of determining the time required to complete a migration.

- Availability of policies and business requirements
- Data availability and accuracy of information about the current environment
- Local resource skills, availability, and co-operation
- Amount of additional infrastructure available to leverage for the migration
- Complexity and diversity of the design
- Change windows and change control process
- Number of sites / buildings involved
- Data volumes

Migration time frames of three months are typical including planning. If you only have three months or less you must be very clear on scope and have adequate resources (physical, people and budget).

- **Who should be involved?**

Although many roles of the migration can be performed by the supplier or third party it is also important for the customer or user to also participate in the migration effort. This should not be restricted to a particular phase, such as the initial planning, or a particular role, such as project management, but across a number of roles and phases. This ensures that there are points of contact and continuity between the customer, the business, and the supplier or personnel performing the migration effort. This helps the communication that is essential during the migration execution and also provides knowledge transfer and similar transitional benefits. These will help the migration be more successful and easier as well as ensuring that the day-to-day operational and support activities needed to operate and maintain the newly migrated environment are known and ready.

The following areas are all recommended for customer or site personnel to collaborate and participate with the supplier or personnel performing the migration effort.

- Management governance and decision-making
- Technical design authority
- Budget governance and procurement
- Support (break fix)
- Operation teams (day-to-day)
- Overall project management (including project governance board)

Depending on the organization structure and size, some or all of these can be contracted out (to EMC or others). A successful migration will require a team effort with a clear understanding of roles and responsibilities and good communication and interaction during all phases of the migration.

- **What are the steps?**

The “Planning” section on page 13 reviews migration steps and provides guidance on the timescales involved.

- **What about the legacy data?**

Legacy backup data is a significant influencing component of any migration and has to be considered regardless of the vendor, size, or any other variables. There are a number of different software products and services that can help in this area, but the options available tend to be limited to three or four strategies. The most common strategies employed for legacy data are:

- *Keep a small legacy data recovery infrastructure.* This is a common approach but difficult to justify and maintain over time. Typically this is only ideal for smaller data restore volumes and retention periods of up to three years.
- *Maintain media (tapes) but contract out the recovery of the data.* This is ideal for some legal or compliance data types where the restore of data is rare and the data recovery volumes are low.
- *Migrate data to a new backup platform.* This is comprehensive and provides optimum speed, protection, and data access; however, it can be very resource- and time-intensive. This should only be undertaken for more strict legal or compliance requirements or where the restore frequency and volumes are expected to be large or time critical.

There are a number of variations to the above and often a combination of these legacy backup data management methods is used. If you have a good understanding of your existing data and the policies that you need to adhere to, this may be an easy question to answer. If you are able to identify and only migrate or protect the data for which you anticipate a restore requirement, it will save time and costs. Regardless of the data policies that you have, it is always wise to look at the diminishing returns of migrating and protecting legacy backup data that may never be needed or that is not important to the business.

- **What infrastructure will be required?**

You should assume that you will need some quantity of new infrastructure for the migration. The amount and type will depend on the capability of the existing infrastructure. A new backup server,

storage node, and some storage devices would be advisable to enable an easier migration process. If no additional infrastructure is used, then this will typically increase the exposure to risks during the migration. It will also increase the time required to complete the migration.

Using additional infrastructure provides the following benefits.

- Less impact to the existing infrastructure, making migration easier and faster to execute
- An easier and faster regression path, which reduces the exposure of any potential risks
- Allows for some work to be completed during production or normal hours, enabling quicker migration
- Enables additional testing and knowledge transfer opportunities
- Increased performance and capabilities that new equipment can provide (faster I/O, CPU, increased capacity, etc.)
- Eases support costs and issues with older legacy equipment

- **How many storage nodes, drives, and servers will I need?**

The amount of hardware resources you will need can be answered only by defining the scope and understanding the current infrastructure and the requirements that are expected to be met. The number of storage nodes, drives, and servers is likely to be less than what is deployed in the current environment due to technology advances and some redesign, assuming new infrastructure is being used; however, this can vary and is subject to the expected requirements for the target infrastructure.

- **Can I use my existing infrastructure?**

You can use existing infrastructure for the migration but you will typically need to have some “float” in order to start the migration. You will also need to be cognizant of the support and requirements of the new backup software and the fact that these are unlikely to match the existing provider.

If the infrastructure is restricted to the existing equipment, with little or no new infrastructure, then it is likely that a number of the possible gains may not be realized. If you choose not to use any new or spare infrastructure, then you risk imposing a restriction on the design and limiting the benefits that can be achieved. This can lead to increased costs and lower ROI and will often result in further costs and effort being required within a short period of time after the completion of the migration.

- **What about my scripts?**

Scripts or other customizations are often used, especially within large or diverse backup environments. If existing scripts provide a unique or custom purpose beyond or outside the capabilities of a typical configuration, then these should be modified to work with the new software wherever possible. If the scripts provide something that can be replicated using a standard backup configuration or application module or API, then these should be used in preference to a script. This eases the support burden from the application and backup providers by simplifying or standardizing the environment.

The following points should be reviewed when dealing with scripts or custom configurations.

- Ensure that you capture all scripts and custom configurations during the design and planning phase so you can review them appropriately and are not surprised during migration tasks.
- Understand what purpose the scripts provide. Is the purpose and requirement valid for the target environment?
- Review available alternatives. If different approaches are easier or provide improved support or performance advantages and meet the requirements, then adopt alternate approaches in preference to custom scripts and one-off configurations.
- Inquire as to how the new solution provider has approached or solved this problem with similar environments or applications. If there is a common module, script, workaround, or methodology, then a new method is worth considering.
- In cases where scripts are used, ensure that they are as simple as possible, are well documented with error handling and reporting, and have a designated owner.

- **What about the people who operate / support the current backup solution?**

Existing backup operations personnel are key to the success of the migration and should be involved at the planning and design phases. They should also be involved in the definition and approval of test and

acceptance phases. The involvement of support and operational teams during the migration improves knowledge transfer, migration speed, and overall success. This is typically limited to a small number of key individuals who cross-train or become mentors for the remaining staff.

Some additional operational and support effort is to be expected during the migration due to the fact that there is additional (new) software being used while the legacy environment is in the process of being decommissioned. This can be provided by the supplier or third party; however, it is more productive and motivating to use third-party resources to back fill and free up support and operational staff for the new environment.

Transitional assurance should also be considered as part of the handover to the support and operational teams. This is likely to consist of some knowledge transfer, during the migration, creation or updates to run books or configuration documentation, as well as formal training.

- **How do we move the backup clients?**

Backup clients are unlikely to be able to be moved in one operation and should typically be grouped into phases. This ensures that the individual phases or groups are of a manageable size and that the configuration and other elements can be planned and understood before the migration is performed.

Here are some tips to help the planning of the clients and the groups or phases.

- Clients should be migrated in groups or project phases to reduce the effort and risk and to accommodate moves within allotted time windows. Small groups should be selected to prove a process or practice early in the migration.
- Clients should be grouped into common areas, such as location or service type, and also be broken into manageable pieces to reduce complexity and effort required.
- Group size should be dictated by the complexity of the client. Simple clients can be migrated in large groups (10 – 100). Complex clients should be done in smaller groups (1-25).
- Complex clients should be managed early in the process and not be left until last. This allows for accommodating changes in time or process, minimizing risk and effort.
- Test and acceptance should be planned and performed for each group. This allows issues to be identified and rectified for remaining clients. It also simplifies the overall handover process and increases the confidence in the target infrastructure.
- Utilize existing technologies such as Microsoft Systems Management Server (SMS) to push the migration process out to the clients.

- **How and what do we test?**

Testing is intended to provide confidence and to validate that a certain condition, criteria, or requirement can be met. Testing should include failure diagnostics and service recovery where appropriate. Decide on the test and acceptance criteria for each group or phase. Simple and low priority clients and groups are likely to require basic or random testing. Complex or higher priority business-sensitive clients are likely to require individual and comprehensive testing.

Complex or custom configurations are likely to justify more comprehensive testing than standard or simple clients. It is important to ensure appropriate and proportionate test and acceptance for migrated clients. However, keep in mind that if comprehensive testing is performed for all clients and services there is an impact on the time and cost of the migration.

- **What about client ABC that takes forever to back up?**

Individual clients or issues need to be identified and analyzed during the scoping and planning phase to ensure that the appropriate decisions can be made.

The poor performance or unreliability may be due to other aspects and may not change or improve simply because different backup software is used. It is important to understand where the problem(s) are and to then look to how they can be addressed or improved.

It is likely that new technologies or backup techniques can be employed to improve the performance of a client following a migration. This, however, needs to be investigated and validated and cannot be guaranteed.

- **What about feature XYZ in the current product?**

Not all backup products look and behave in the same way. It is therefore possible that some features will not be exactly the same between any two products. The scope and planning phase should identify these features differences and allow for decisions to be made on how to address requirements met by features of the former solution.

Notes to consider when looking at these features include:

- Do not focus on the feature, focus on the requirement that it is fulfilling. Is this a requirement that the business needs? Can it be met via an alternative process?
- Design to the strength and the architecture profile for which the backup product or device has been designed.
- Consider how the environment will scale and perform over time. Are you imposing restrictions on future scale or performance?
- Ask the solution provider how they have approached or solved this problem with other similar environments or applications. A common process or methodology is likely to be better from a support, scale, and performance perspective.
- Consider how the environment will be managed. The ability to report, monitor, and analyze the environment is a critical element to consider. Anything that limits or makes this aspect more difficult can have repercussions and generate hidden and ongoing costs.

Planning

The most important part of any migration is likely to be in the early stages where the planning and various key decisions are undertaken. These plans provide the foundation and boundaries for the migration and therefore define the cost and benefits that are to be achieved. It is therefore important to ensure that enough time is allocated to planning and that the steps used ensure that the appropriate level of detail is gathered. This detail will be used as the basis for the design and any decisions made regarding architecture, scope, or scale. The following list is a suggested order for steps or milestones typically used during the planning phase.

- Determine scope
- Establish objectives
- Collect all requirements
- Estimate time and effort
- Produce a list of costs
- Produce a proposal
- Refine the proposal
- Agree on the preliminary scope, objectives, time, and costs
- Gather detailed data and further analysis
- Ratify the proposal and build the design and project plan
- Confirm the final scope, objectives, time, and costs
- Execute according to the design and project plan

Delivery

The delivery phase continues with the planning but concentrates on applying basic reporting, communications and control. This is where the project manager or the infrastructure or delivery project manager is normally fully engaged. Once the basic control and communication are established, the resources and detailed planning activities can start. These will include delivery of equipment, scheduling and confirming resources, and submitting work permits, delivery forms, or initial change requests. The execution of the design includes a large number of activities, a number of which may be able to run in

parallel. There will also be a number of dependencies that all need to be accounted for as part of the execution. The following list is a suggested order for a number of milestones or considerations that are typical of a delivery phase.

- Execute the design according to the project plan
- Use a phased approach
- Minimize risk (Keep it simple)
- Use / involve operations and support
- Test
- Control change (minimal, good reason)
- Update design and documentation
- Validate process during the migration
- Ensure knowledge transfer and training
- Handover (transitional assurance)
- Record observations and recommendations
- Agree upon follow on actions

The delivery phase is very specific to each unique customer. A number of the aspects of the delivery phase are dependent on the detail, thought, and time applied during the planning and design phase. This can have a major impact on the time and the number of issues or changes that are encountered during the delivery phase. Even in cases where the planning and design were well prepared, it is expected that some issues and change are likely. These should be handled using the appropriate project management methodology and control. This will ensure that issues are not only resolved quickly, but that they will also be resolved using the most appropriate method and recorded and communicated appropriately.

In the case where multiple project managers or teams are involved, it is recommended that a single project manager and project board are used to coordinate all tasks and teams. It is typical for the delivery to involve the supplier, the customer, and at least one third party during the delivery phase. All of these parties need to communicate with one another and with a common control and management entity. This should be the role of a single project manager who also reports to or is a member of the project board.

Execution and timescales

The amount of time and the steps required to complete a migration can be significant and challenging in both technical deployment and planning complexity. With the appropriate time, skills, resources and project management, migrations can, however, be achieved with minimal disruption and deliver significant advantages for many years.

Migrations take time to complete; however, there are a number of ways in which this can be controlled and effort can be minimized. This includes simple steps like reducing the scope to fit within a specific budget or timescale. Alternatively you can focus on a particular location or problem area in order to realize the maximum value to the business. The following are some areas that can either increase, or be used to limit the amount of time, effort, or cost of a migration as well as some other considerations.

- Planning should be extensive (at least 20 percent of the time to migrate)
- Time constraints impose restrictions on execution and design
- Infrastructure constraints impose restrictions on execution and design
- Training and knowledge handover must be included
- Processes will change
- Communication and project control ensures success
- Testing and sign off (handover) are keys to success

Migration execution and timescale will vary for all of the reasons mentioned here. Figure 1 provides guidance on the typical steps and order of a migration. It shows an indicative timescale that could apply to these steps. These times act as a guide and are typical of migrations in which EMC has participated; however, your actual timescale will depend on your particular situation.

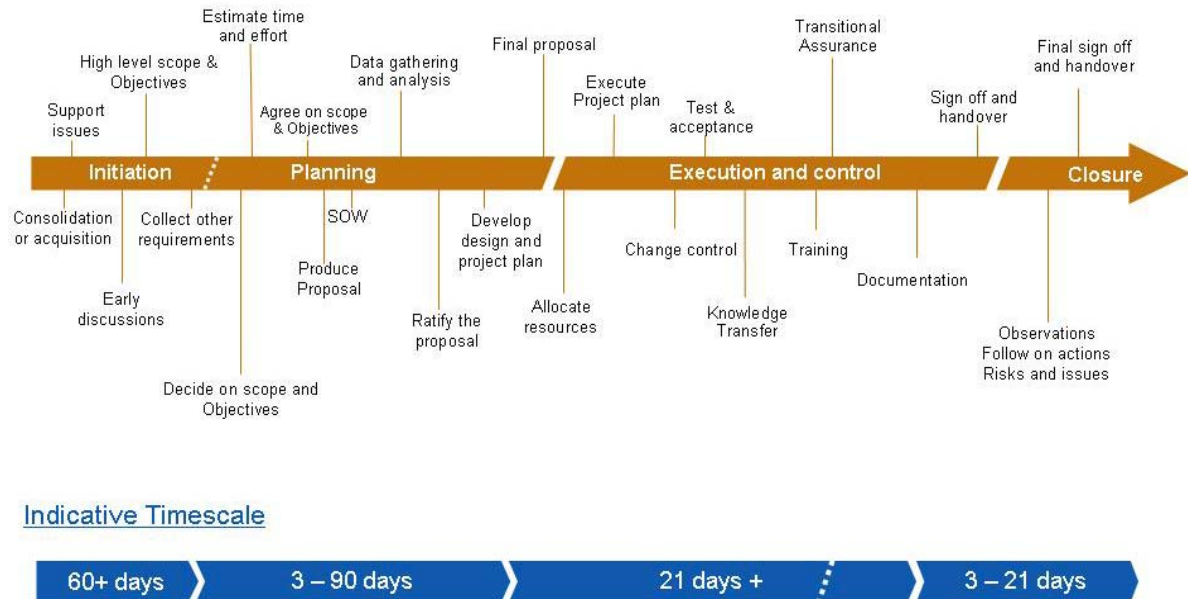


Figure 1. Migration steps

Conclusion

There are many benefits of simplifying your environment through backup consolidation. This can involve consolidation from a number of different products to a single product or a swap from one product to another. Updating your backup and recovery software affords you the opportunity to understand, control, and improve your data protection environment. This can result in significant cost savings in operational effort, support, and future growth. It also enables you to improve your service levels, increase performance, and establish a data protection solution that grows with you.

This paper details many aspects and considerations of consolidation and moving from one backup provider to another. It highlights how consolidating your environment can be achieved and that budget, resource limitations, and risk concerns can be managed when the right people skills and processes are used. Consolidation has many benefits and can very quickly provide benefits and real cost savings. This information has been gathered from EMC's own experience working with and supporting a large number of customers as they transition solutions.

With solutions including NetWorker, Avamar, EMC Disk Library, and RecoverPoint, EMC brings you the latest technologies including backup-to-disk, deduplication, snapshot management, continuous data protection, up-to-date application support, and advanced environment reporting and analysis. If you are considering a shift in your backup and recovery strategy, EMC can carefully guide you through the entire process, from design to implementation and sourcing the right set of technologies.