Online Backup Solution
Presented for The Digital Ranch

Presented by Jacob Beebe and Zach Howlett
Introduction
We sat down together and set some project goals for what we wanted to do for our masters project. The goals are below:

- Gain Real Word Experience,
- Enhance Resume,
- Provide a Service for a Local Company,
- Network with Peers in Industry, and
- Graduate from the program.

The online backup solution project is to research and find a solution that the Digital Ranch (“the Ranch”) could offer its customers as a Managed Service Provider (MSP). This project consisted of the following six parts:

- Project Plan,
- Market Research,
- Product Research,
- Product Selection,
- Installation/Testing, and
- Conclusion/Reporting.

The project came about because Zach had previously done an internship with the Ranch and had a friendship with Steve Burton and Andrew Yenchick. Zach approached the Ranch and asked if they had a project that he and his masters group could work on for their final project. The Ranch was looking to offer its customers an online backup solution.

The Ranch wanted research done on online backup solution that it could offer its customers. The Ranch did not have the time or resources available to do this research on their own. The Ranch wanted Zach Howlett and Jacob Beebe (“we”, “us”) to research and test specific products that met certain criteria for what it was looking to offer its customers.

The Ranch was to provide the hardware and operating systems for testing the software packages. We were to obtain the software packages from the distributors on a trial basis to test the two software packages that best met the criteria that we established and the Ranch modified and approved.

We started the project by coming up with a project plan. As we learned in the Project Management class, without a proper plan in place a project can doom for failure from the start. After we created the project plan, we were able to see how the project would lay out.

Project Plan
We started our planning of the project by identifying the key stakeholders of the project. They were as follows: The Digital Ranch, The University of Utah MSIS program, Jacob and Zach, and The Ranch’s customers. By identifying who the key stakeholders were for the project, we were able to put into perspective the goals and desired outcome of the project.

After our meeting with Steve, we put together a plan that we thought would help guide us through the entire project. The project plan consisted of the six parts listed above.
Market Research
We wanted to start our research by finding out if the Ranch is getting into a good market by trying to offer its clients an online backup solution. However, the market place might be a little skewed because the Ranch is looking to offer an online backup solution more to its existing customers than new customers for the time being. As our research shows, the barriers to entry to the market are low, especially in Utah. We did a quick Google search looking for local companies who offer online backup solutions, and were able to determine that the competition seems small. There were out of state companies listed on the first page of searches for Utah companies. This tells us that either the competition in Utah is small or that the competition is not advertising their product well. This can lead to a good opportunity for the Ranch to enter the market. Our market research is below.

The following graph describes the main causes of data loss. Although the graph is from 2002 and can be argued that it is outdated, it is the most recent graph we could find. From our research about data loss, we concluded that most recent research of data loss seems to be focused on data loss that occurs due to a breach. We thought that by including that type of research it might be misleading, rather than offering a fair comparison.

As you can see from the graph, 76% of data loss either occurs because of human error or hardware malfunction. (AhSay) Hardware failure and human error are going to happen in every company. To help protect a company from the damages that are incurred by data loss, a backup plan needs to be in place. Whether a company wants to control their own backups or outsource the service is a business decision that each individual company must make. A survey in 2011 found that over 50% of businesses lost business data. 10% of those companies could not recover their data. 27% of companies stated it would take about 24 hours to recover their data.
These are alarming statistics. Also in the StorageNewsletter.com survey “45% of those surveyed found their data backup solution only 'moderately effective' while 22% believe their current data protection is ineffective.” That means that 67% of companies do not feel safe with their current backup solution.

This means that the market for an online backup solution should be strong. If half of companies lost data, and two thirds are not comfortable with their current backup process, the Ranch can fill the void and help these companies. When companies lost data the costs that are associated with it are: the data itself, employee compensation for restoring the data, cost of hardware failure, cost of company inefficiencies, cost to pay an outside vendor to restore data (if needed,) downtime for company (if applicable,) and reputation. Some of those costs are easily attributable, while others are not. It has also been noted that 60% of companies that lost data go out of business within 6 months of the loss. (Data Loss Statistics)

Another concern for businesses is that laptops are increasingly used for travel and in-office use. Data loss is more likely to occur with laptops. The laptop is usually being moved from place to place which increases the chances of hard drive failure. Also, laptops are more likely to be lost or stolen. The costs of data loss vary by study. In 2003 a study by Pepperdine University found that the average cost of data loss is $3,957. The breakdown is shown in the graph below. (DAVID M. SMITH, 2003) The Pepperdine study found that data loss costs businesses $18 billion dollars a year.

Other studies have produced numbers that are a lot higher. The StorageNewsletter.com survey found that the average cost of a broken or stolen laptop is $25,000. "A survey conducted in 2001 by Contingency Planning Research reports that the majority of companies estimate the average cost of computer network downtime to exceed $50,000 an hour, and for some companies that figure rises to over $1,000,000 per hour." (Armour, 2006) We feel that number is more geared towards large companies.

With all this data about the costs and concerns of corporate data loss, we found that the market to enter for the Ranch is reasonably open. Below is a graph produced by Forrester Research. (Dines, 2010)
This graph indicates that 79% of small to medium businesses (SMB) either are not interested or don’t have plans to offer Backup-As-A-Service or online backup services. 6% of firms who offer the service, do not plan on expanding their service. This leads to an opportune market for the Ranch to develop. Currently, the Ranch is more looking towards offering this service to existing customers, but if they want to pursue further market involvement, it would be a wise decision.

**Product Research**

After determining that the market was viable for the Ranch, we wanted to go about choosing a product that made sense financially for the Ranch as well as delivering the advertised results. During the planning phase, we created some criteria to narrow the field of possible software solutions. The criteria we used to narrow the field are below:

- Research industry leaders,
- Weed out consumer products (we were looking for a MSP product,)
- Research forum and review websites (we were looking to eliminate products with multiple issues regarding functionality. If a product had multiple pages and issues we eliminated them from our pool,)
- Research competing products, and
- Narrow the field to 5 products for evaluation.

During the planning phase, we created a software selection matrix. The goal of the matrix is to be able to distinguish different software packages based upon pre-determined standards. After we created our initial matrix, we sent it to Steve at the Ranch for review. We wanted to make sure that our client (the Ranch) was able to give input on what they deemed most important in the software selection process. The numbers in the matrix are the associated values given to each product feature.
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Weight (example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incremental Backups</td>
<td>(0.15)</td>
</tr>
<tr>
<td>Compatibility (cross platform/OS version)</td>
<td>(0.15)</td>
</tr>
<tr>
<td>Scalability</td>
<td>(0.10)</td>
</tr>
<tr>
<td>Ease of use</td>
<td>(0.15)</td>
</tr>
<tr>
<td>SSL security</td>
<td>(0.10)</td>
</tr>
<tr>
<td>Password protected</td>
<td>(0.05)</td>
</tr>
<tr>
<td>Encrypted Storage</td>
<td>(0.15)</td>
</tr>
<tr>
<td>Whiteboxing</td>
<td>(0.05)</td>
</tr>
<tr>
<td>Price</td>
<td>(0.10)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1.0</strong></td>
</tr>
</tbody>
</table>

After establishing the numbers above, we were able to narrow down the number of companies to focus on and do more research. The companies on which we chose to do more research were Asigra, NovaStor, Vembu Storgrid, Syncrify, and Ahsay.

**Asigra**

Although Asigra is the industry leader in online backup solutions and has the best product features out of all of the companies we looked at, the price of using Asigra is well outside of the budget, eliminating it from the options. The options and features Asigra offers are geared towards large to enterprise level companies. The real advantages of their product are best seen in large installations involving numerous workstations, multiple servers and databases, higher security levels, and storage solutions around 100 TB or larger per client.

Asigra uses an agentless DS client installed on the network that can back up the entire business. This reduces the security and performance risks of having additional applications installed on database and web servers, unlike every other software package. Due to one client backing up an
entire network, the DS client can also track duplicate files saved on multiple computers and save pointers instead of the files. It can also track repeating blocks within files to give Asigra the best compression rates and lowest storage size of all the software options. Clients will also be able to run initial full backups to external media and ship them to the backup service site instead of requiring days to transfer it over an internet connection. Backups will still be fully encrypted and protected during transit. They were also the only software package that can backup and cover mobile devices, such as smart phones and tablets.

Asigra uses a capacity-based licensing system that costs between $2000-3000 depending on if it is in an online or archived data storage setup. The cost of buying licenses for 150 TB would be over $400,000. The benefit of using a capacity-based license is it allows multiple DS client installations on the client network for redundancy and load balancing the workload at no additional fee. We felt that the price alone is enough to eliminate this option from further inclusion in the decision process. Asigra doesn’t provide the best match for the market to which the Ranch is looking to supply.

**NovaStor**

Novastor actually provided a good match for the Ranch with two Notable problems. The initial upfront cost of using Novastor includes a $5000 initialization fee besides a monthly flat fee of $3 per client per server license. The upfront costs include a Novastor rep visit for installation and branding, but we still felt this was a high starting point for the Ranch. Even considering the $5000 as a sunk cost, the perpetual fees are higher than some of the other options, making it less profitable in the long run. Novastor is also only compatible with backing up Windows and Linux based desktop/laptops which didn’t match the cross platform compatibility we needed. They did have all of the required features and security protections. Novastor stood out as the product with the best technical and sales support. Their offices and support team are based out of California and can be reached during business hours. Even during a call with a sales rep, we were able to talk directly to technical support engineers to have all our more detailed questions answered. Novastor is also the most scalable, with the ability to add additional server side clients which can load balance, and client scalability at a flat rate. Novastor was also the only licensing-based software that didn’t include additional feature fees for things such as backing up VMware or HyperV image backups. We also feel that Novastor would represent savings in fewer man hours dealing with any product/technical issue that requires vendor support. The Digital Ranch wanted to start in the market place and offer a very limited amount of online backup storage and user licenses. Novastor requires a much higher up-front costs and higher perpetual costs/license for clients and servers which makes up the majority of the predicted client usage. If The Digital Ranch ends up mostly supporting servers and virtual images over time, this product might have been a better solution than Ahsay.

**Vembu Storgrid**

Vembu Storgrid is an online backup solution that offers a variety of features. Storgrid can be cloud based which is something the Ranch thought they might look into in the future. If you become a Vembu partner, they offer free training and marketing help to get more customers. They fly a representative out to help the partner set up and install the system.

Vembu did not have an additional charge for different types of services that it backs up such as Exchange and different databases. It also comes with the ability to back up entire networks. Vembu has some limited branding features. You can input your own information, but you
cannot fully brand the product. Another issue with Vembu was that it does not support Mac backups.

As far as a feature set, Vembu would be a great product for the Ranch. It offers all the features they are looking for and seems to have a very reputable product. The reviews online are very positive for Vembu. However, the main reason we feel this would not be a good product is the price. Just to start, Vembu requires $2,000 in up front costs. That does not include the additional licenses that have to be purchased for each client that is to be backed up. In comparison to Ahsay, Vembu licensing fees were very expensive. Vembu was eliminated mostly based on the costs associated with the product and the limited branding features. (Vembu NovaStor, 20111)

**Syncrify**

From the start of our research, Syncrify was one of our favorite products. By reviewing their website, we determined they had every feature that the Ranch wanted in a product. Also, the pricing by far the cheapest product we found. However, their website is a little basic compared to others in the industry.

Syncrify works and has installs for all operating systems, including free BSD. It offers encryption on data. Syncrify has the capability to brand both the client and the server with their ISP edition. Also, Syncrify uses SSL to transfer the backups across the internet. The ISP edition of Syncrify costs $1,500 and comes with 100 licenses.

Syncrify claims that it is a product and not a service. Therefore there are not any fees associated with it except the purchasing of licenses for the product. Syncrify has two different types of products that it sells, a Professional License and an ISP license.

Syncrify uses the rsync algorithm to backup files of the user’s choosing. Rsync is a way in which files are compared and it is determined what parts of the file have been modified. After an initial backup, Syncrify will utilize rsync to determine what needs to be backed up and what files have not been changed since the previous update. Syncrify utilizes what it calls a delta backup that will only backup the parts of a file that have changed and not the whole file if it has changed. Therefore if you have a 1GB file and only 5MB change then Syncrify will only backup the 5MB and not the whole 1GB file. Also, before files are sent across the network Syncrify utilizes what it calls a smart compression. That is, if a file can be compressed before transmission it will be, however, if a file cannot be compressed it will be sent whole.

**Ahsay**

The best software solution for what the Ranch wanted to offer to its customers is Ahsay. The pricing model that Ahsay uses is affordable for a MSP to grow a backup business geared towards small or medium business solutions. Ahsay supports full and incremental backups, multiple backup schedules, all major OS platforms, desktop/laptop/server client applications, and all major feature applications such as VM and Hyper V Images, all major databases, bare bone backups and exchange services. An OBS client (server side) is installed as an application on a server, or Ahsay also offers its own server OS. Ahsay is very scalable, with the ability to add additional OBS clients and OBS replication backups for free, and client licenses can be increased at any time.
Ahsay supports both encrypted storage and SSL encryption. Password protection can be enforced and passwords aren’t stored on the backup servers. Ahsay also allows for complete white boxing so the Ranch can have only its name and branding on the products that the customers see. The software also offers offline backups to removable media and a local copy feature for customers that require faster restore options. Ahsay offers purchase or lease options and only charges for client side licenses. Note that additional fees are for Exchange boxes, Virtual machine backups, and RDRs. One of the few downsides of Ahsay is that they are based out of Hong Kong so they are not available during business hours unless an appointment is scheduled.

Ahsay had some legitimate negative reviews for the amount of time it takes their technical support to address problems, but they still had a very high approval rating from users in the forums. The internet research was initially misleading with bad press about Ahsay. A Google search returns “Why I switched backup software from Ahsay to Asigra” as the 5th result and “Ahsay raising prices by 700%” as the eighth result. The first being a blog on a website which looks like it is a marketing ploy from Asigra to discredit Ahsay (they didn’t do a very thorough job with obvious business flaws). The second Google link represents inaccurate information about an increase in the lease price for OBM (client server) licenses. The real increase was from around $3.5 to $6/month, not the $27/month lease fee the post claims. This just goes to show you that you have to take information from the internet with a grain of salt at times.

As the backup business grows, additional purchases can be made like a RDR which is a front end load balancer that will support and direct backups to multiple OBS servers, but that is only recommended for businesses that have over 1000 current client licenses. In short, Ahsay offered everything the Ranch was looking for. Not only does Ahsay provide all of the features and functionality the Ranch desired, they also have the smallest start-up costs and the lowest overall costs, making Ahsay one of the more profitable options.

**Product Selection**

After doing all the research for each individual product above we gathered all of the information we had and sat down to discuss how each product scored on the product selection matrix. When coming up with the numbers for each section we should note that a considerable amount of discussion took place on the pros and cons of each attribute. From this discussion we were able to come to a consensus on what the number should be. After doing research on each product we became aware that most products have a very similar feature set. Cost would become an increasingly important consideration as the Ranch was not looking to pay a large sum of money up front. They were more looking to start offering online backup solutions to their existing customers and not fully engulf themselves in the market.

Below is the completed software selection matrix. As you can see the two products that scored the best were Ahsay and Syncrify. The two products with the highest scores means that they are most what the Ranch is looking for and the products that we will install and test the functionality.
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Weight</th>
<th>Ahsay</th>
<th>Novastor</th>
<th>Vembu</th>
<th>Syncrify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incremental Backups</td>
<td>(0.15)</td>
<td>.15</td>
<td>.15</td>
<td>.15</td>
<td>.15</td>
</tr>
<tr>
<td>Compatibility (cross platform/OS version)</td>
<td>(0.15)</td>
<td>.15</td>
<td>.08</td>
<td>.08</td>
<td>.15</td>
</tr>
<tr>
<td>Scalability</td>
<td>(0.10)</td>
<td>.10</td>
<td>.10</td>
<td>.07</td>
<td>.10</td>
</tr>
<tr>
<td>Ease of use</td>
<td>(0.15)</td>
<td>.12</td>
<td>.15</td>
<td>.15</td>
<td>.15</td>
</tr>
<tr>
<td>SSL security</td>
<td>(0.10)</td>
<td>.10</td>
<td>.10</td>
<td>.10</td>
<td>.10</td>
</tr>
<tr>
<td>Password protected</td>
<td>(0.05)</td>
<td>.05</td>
<td>.05</td>
<td>.05</td>
<td>.05</td>
</tr>
<tr>
<td>Encrypted Storage</td>
<td>(0.15)</td>
<td>.13</td>
<td>.15</td>
<td>.15</td>
<td>.13</td>
</tr>
<tr>
<td>Whiteboxing</td>
<td>(0.05)</td>
<td>.05</td>
<td>.05</td>
<td>.03</td>
<td>.05</td>
</tr>
<tr>
<td>Price</td>
<td>(0.10)</td>
<td>.10</td>
<td>.05</td>
<td>.05</td>
<td>.10</td>
</tr>
<tr>
<td>Total</td>
<td>1.0</td>
<td>.95</td>
<td>.88</td>
<td>.84</td>
<td>.98</td>
</tr>
</tbody>
</table>

The results of the matrix showed that Syncrify is most compatible with the Ranch’s requirements as a software package. Will the installation/testing of Syncrify and Ahsay yield the same results as the product research?

**Installation/Testing**

Before we started testing each application, we came up with a testing plan in order to standardize the testing we were going to do. We broke the testing phase into the following sections:

- Setup Hardware/Install Software;
— Run tests tracking results, performance, and errors; and
— Select a software that best fits the Ranch’s needs.

We then created a testing plan that included procedures for what and how we are going to test each application. We then sent what we compiled to the Ranch to verify that we are testing what they want us to test. Below is the testing plan we sent and had the Ranch verify. We broke down the testing into two categories: compatibility and functionality.

**Compatibility Testing:**

- **Types of Files:** pdf, doc, xls, ppt, config files, avi, index.html, images.
- **Types of Services:** database (MySQL), MSSQL, mail server, (possibly exchange server)
- **Types of Platforms:** Mac, XP, Windows 7, Server 2008
- **Web Browser Testing:** Safari, Internet Explorer, Firefox, Chrome

**Functionality Testing:**

- **Backup Scheduling:** complete a full backup followed by scheduled incrementals. Does the scheduling work (daily, hourly?)
- **Types of Backups:** backing consisting of a small number of large files, backup consisting of large number of small files, combination of both (barebones backups available – how well they work?)
- **Backup limits:** can a client backup data larger than their allocated space?
- **Management During Backup:** can admin user control the live backup process (pause, restart, stop, change backup set?)
- **Simulated Backup Interruption:** interrupt a scheduled backup and see what happens (computer restart, network failure.)
- **Backup Completion:** if a backup is not completed, what happens?
- **Offline Backup:** complete an offline backup using external storage and sync it to client account.
- **Restore Testing:** is the data that is backed up usable and complete?
- **Security:** the type of security used to protect the data – when backups are transferred and how they are stored on the backup server.

The Ranch expressed the need for documentation with us. The last group that did their master’s project for the Ranch could not always say how they fixed problems and came up with solutions. We decided that the best policy for the project is to document everything. Our main source of documentation was to take screenshots of performance and settings we used for backups. We also decided to keep detailed notes on how we were setting up certain backups and how we were solving issues as they arose. Also we wanted to provide the Ranch with administrator guides that we found so if they decided to use the product they would not have to search on the internet for it. We created installation guides for both client and server installations that they could provide to their customers or use to set up their servers.

**Syncrify Testing**

Installing Syncrify server was very easy. The download package can be found on Syncrify’s website for free. After the application is downloaded a simple install wizard guides the user through the setup. The only hiccup in the server installation was to be able to get the correct ports open for Syncrify to work. Syncrify by default uses port 5800. After setting the firewall
the server and the client that we were trying to connect to the server we were still unable to connect. It was frustrating for a couple of hours as we tried multiple different fixes and solutions before we realized that by default the Ranch has their firewalls set at “deny all.” Once we asked the Ranch to open port 5800 we were able to connect. The client install is found on the Syncrify servers website, as shown below. Once the client is downloaded, a setup wizard makes the installation very easy.

We installed the Syncrify server on a test machine that the Ranch let us use. The server’s specifications were as follows: Windows Server 2008 R2 SP 1, 1 GB of RAM, AMD Athlon 64 X2 Dual Core Processor 2400+ 2.20 GHz, 64-bit OS, T1 connection. We installed the client application on Windows XP, Windows 7, and Mac OSX.

**Compatibility Testing**

We tested web browser compatibility on both the client and server side. For the browser testing we went to Syncrify’s website and clicked on all the links and tried all the features that were available. We also used the site as a user would to test for functionality. On the client side we tested using Internet Explorer, Mozilla Firefox, Google Chrome, and Safari. On the server side we also tested Internet Explorer, Mozilla Firefox, and Google Chrome. There were no issues noted during the testing of the web browsers.

**Mac Compatibility**

A Syncrify Mac client can installed from the Syncrify server. The Syncrify web portal did not have any issues with Mac. We did the same testing for Mac as we did for Windows and nothing was different. We tested web compatibility for Safari, Google Chrome, and Mozilla Firefox. The Mac application did not have any issues. We tested every link and feature on the application and found nothing that would make us think that the application would have functionality issues in the future. The picture below is of the Mac client when setting up the connection between the server and the client machine.
Functional Testing

Backup Scheduling
The Ranch wanted an online backup solution that would run automatically when a schedule has been set. This allows for minimal administration needed once the schedule has been set by the client. Syncrify allows for a schedule to be set at the following intervals.
The schedule is set for the incremental backups that occur after the initial full backup has taken place. Also, Syncrify allows the clients to be backed up in minute intervals.

![Screenshot of advanced schedule options](image)

We did not encounter any errors with Syncrify’s scheduler. Every time a backup was scheduled to run, it did. We even planned skipping scheduled backups to see how the program responded. When a scheduled backup is missed, the next time the client is online the backup process will resume immediately. We tested this by having a client turned off during a scheduled backup. Once the client was turned on, one of the first services to start was Syncrify. We tested this multiple times and each time the process started immediately. Below is a screenshot of the schedule that was setup as it appears in the Syncrify client.
Types of Backups
We decided to test multiple different types of backups in order to test how the client reacted towards backing up different sets of data. We wanted to encompass how future clients of the Ranch would backup their data. As noted earlier, our backup procedures were approved by the Ranch. The backup types we used were as follows: backups consisting of a small number of large files, backups consisting of a large number of small files, backups consisting of a combination of both. The Ranch wanted us to perform a bare metal backup, but Syncrify does not have the functionality to perform such backups. Syncrify did not have any issues either doing a full backup of a large number of small files or completing the incremental backups for these files. The client worked exactly as advertised.

However, during the backup of large files, Syncrify sometimes got hung up and froze. The client would not complete the backup process. The backup process was left multiple times when a freezing had occurred to sit for over 24 hours to see if the problem would correct itself. The process did not ever correct itself. Also, there was no notice sent to either the administrator or the client when the backup failed to complete. Once the process was killed and the service restarted the backup would start over from the beginning without starting from where the previous backup failed to complete. We researched many different types of fixes for this stalling of files and could not find a definitive answer for why this occurs with Syncrify. Multiple different fixes were tried, such as clearing out configuration files from multiple different folders to try and solve the issue. There was also no rhyme or reason for why a backup of a large file would complete or freeze. It was more or less the luck of the draw. A part of the problem could have been the T1 connection and that the internet connection that was allowed was too slow to process the encrypted information we were trying to backup.

We were really surprised at the results of the testing in this area. We did not think this was acceptable to offer to clients. If a company is going to offer the service to customers, it needs to work all the time during the testing phase or fixes need to be found. This was not the case with Syncrify.

Backup Limits
At the time of client setup by the administrator, each client is allocated a certain amount of space that they have to backup data. The amount that is allocated can be changed at any time. We tested what would happen if the amount backed up by the client exceeded the amount that was allocated for that client by the administrator. If this occurs the client backup will complete even if the space allocated is less than the backup. No messages were sent to either the administrator or the client if this happened. However, if the administrator goes to the “Manage Users” section in the web portal they will see that the user’s information is displayed in red meaning that the client has used more space than they were allocated.
The next time a client tries to perform a backup an error message pops up that says something to the effect of “backup space allocated has been reached. In order to complete a backup contact your administrator.”

**Management During Backup**

The Syncrify application has very limited management features. Administrators can set allocated limits to clients, create clients, and a couple of other features. As far as management during a backup, all an administrator can do is restart the entire Syncrify service or shut it off. An administrator cannot pause a backup process or set bandwidth limits to each client. Because of this limited feature set, the administrators have very limited control over the client and how they choose to use the service.
Simulated Backup Interruption
We wanted to test how the application would respond to a simulated backup interruption. We performed the following tests to the Syncrify client to see how it would respond to a network interruption:

- Turned off internet connection,
- Restarted Computer, and
- Interrupted backup by moving computer to a different network.

In the first test we turned off the internet connection on both the client and the server. After we let a period of time pass we reconnected each machine. Upon reconnecting to the Internet, each backup instance was able to resume from where it left off. In each testing instance the backup completed successfully.

In the second test we restarted the client machine to test if the backup would be able to complete. In each case the backup was able to resume where it left off. In the third test we took the client machine and moved it to a different network. In each instance the backup completed successfully. In conclusion, Syncrify performed very well when a backup was interrupted and in each case the backup was able to continue and finish successfully.

Backup Error Notification
Syncrify has a feature allowing you to email reports to both the administrators and clients. However, after setting up email alerts for both backup errors and completion we never received an email notification. We tried multiple different fixes and email addresses to test to see if a notification would be received. When backups would fail, no notifications were sent to either the
client or administrator account we set up. Below is a view of the email account we used to test for the client.

![Image of email account]

**Restore Testing**

Syncrify has built-in feature that allows for restoration of previous backups. The restore process does the following:

![Image of warning dialog]

After we clicked yes to the above screen we needed to input the encryption password for the data we wanted to restore. If the password was incorrect the restore process could not take place.
We moved the folder that the client backed up and move it to a different location on the local machine to test the restore process. Syncrify does allow for multiple different incremental backups to be saved. The restore process did work correctly. We compared multiple files after the restore was complete to verify that the restore worked correctly. In all cases the restore was successful.

**Security**

Encrypting data is not a default option in Syncrify. However, if the client chooses to encrypt its data (the Ranch said would be mandatory) Syncrify uses AES 128-bit encryption before the data is sent across the internet. We tried to access the data that was stored on the server by both the administrator account and the actual data that was stored on the local hard drive. In both instances, the data cannot be accessed as it is encrypted. When a file is opened, an error message comes up saying that the program cannot access the document because it is in format that is unknown or the file is corrupted. Then, only way to access the encrypted data is to unencrypt either the file or folder in the Syncrify application.
The user sets the encrypted password. If the password is lost or forgotten there is no way to recover the data unless the user uses a weak password. Also, if data is encrypted and the user wishes to change the encryption password they must remember the previous password or else they will not be able to access the previous data they encrypted. The administrator cannot reset or change the encrypted password. Also, we tried to capture packets using Wireshark to see if we could recover a file but the packets were all encrypted and unreadable.

Another form of security Syncrify has built in by default, is that administrator access cannot administrate functions outside the actual physical machine Syncrify server is installed on. In order for administrators to access the admin console, they either have to be on the local machine or have remote access to the machine. The administrator can change the feature to be able to access the administrator section through the web portal. All network traffic via the web portal is done over HTTPS and encrypted for both the client and administrator.

**Syncrify Branding**

Syncrify advertised that both the client and the client web portal were able to be fully branded. However, after branding the client and the web portal, Syncrify’s branding was very basic and didn’t work as the Ranch wanted. The Ranch gave us a couple of images that they wanted us to test the branding features. Below is a picture of the client application that was supposed to have a banner ad where the red bar is. We could not get the banner ad to work.

On the web portal, Syncrify’s label was all over the place. The Ranch wanted branding for their client to see only the Ranch’s logo. We tried to place an image on the web portal but it did not
work. There were no fixes available. Below is a picture of the client web portal with Syncrify's label but not the Ranch's as we tried to do.

![Client web portal](image)

**Performance**
The following statistics are the performance we achieved when we were testing Syncrify. Below are the testing results for a full backup. We believe the main reason behind the length of the backups is that we were backing up large amounts of data over a T1 connection.

We backed up 3 types of data sets:

Small <1 GB. These backups usually took between 0-2 hours.
Medium 1-5 GB. These backups usually took between 5-12 hours.
Large >5 GB. These backups usually took anywhere from 14-28 hours.

The following are the times it took to do incremental backups:

Small <1 GB. Backups took between 15-30 minutes.
Medium 1-5 GB. Backups usually took between 1-4 hours.
Large >5 GB. Backups usually took between 5-8 hours.

**Ahsay Testing**
Ahsay equips a full range of enterprise-class features for backing up data stored in virtual machines, database servers, email servers, file servers, desktops and notebooks. Its OEM Edition is designed to empower MSPs to provide secure online backup and disaster recovery services to their business customers. The software is divided into two main subgroups: Client side and Server Side applications.
Ahsay™ Online Backup Manager (AhsayOBM) is a client-side backup application bundled with comprehensive backup features and specialized backup modules for backing up VMware and Hyper-V virtual machines, Microsoft Exchange Server, Microsoft SQL Server, Oracle database, MySQL database, Lotus Domino/Notes email system, Microsoft Outlook / Outlook Express, Bare Metal Backups, Windows System State, Local Copy of Backups, etc. It is thus ideal for backing up application servers, email servers, and file servers.

Ahsay™ A-Click Backup (AhsayACB) is a light version, client-side backup application with clean and easy-to-use interface designed for general users to back up Microsoft Outlook/Outlook Express and common files in Windows/Mac desktop and laptop computers.

Ahsay™ Offsite Backup Server (AhsayOBS) is the core server-side application for offering centralized backup services to AhsayOBM and AhsayACB client users. It is used for managing individual users and their account configurations, as well as monitoring the entire backup system’s performance. The AhsayOBS server machine can be placed onsite as well as offsite. In addition, you can run AhsayOBS application on a cloud platform for cost saving purposes.

Ahsay™ Replication Server (AhsayRPS) provides an offsite store for backup data from one or multiple AhsayOBS servers. Data from AhsayOBS will be replicated almost instantly after a backup job is completed. It thus provides an additional level of data protection. When disaster strikes, you can either convert the AhsayRPS into AhsayOBS for keeping the backup uninterrupted, or restore the replicated data back to the AhsayOBS for disaster recovery.

For a standard installation, a partner would first purchase licenses and create a partner account with Ahsay. Once the account is created, the partner would then log into the customization portal on the Ahsay website where they would be walked through the different options on how to brand the product with their own logos, graphics, and phrasing. Branding will be covered in more detail later on. Then the partner would then be able to download the customized Ahsay OBS and RPS application for installation on the designated backup server.

Compatibility Testing
The Ranch provided a test machine to use for the backup server on their network. The server specifications were as follows: Windows Server 2008 R2 SP1, 5GB of Ram, Intel Pentium 4 Processor 3.00 GHz with Hyper Threading, 64-bit OS, and a T1 internet connection with a bandwidth restriction of 1Mb/s placed on the connection at the firewall. Server installation was very fast and easy. Only default language, time zone, default port selection, and installation location are required to install the product.
The Ahsay OBS server uses ports 80 and 443 for the default configuration which works well with most business firewall access. Custom ports can be selected and used if desired. Ahsay OBS is a web portal installed on the backup server that clients can navigate to. Clients would then select from either the OBM or the ACB download and installation wizard from the left side of the screen.

A new web page then opens allowing the customer to select which OS platform they are using by selection one of the graphics at the top of the window. The page changes with the selection to give the customers the correct download package and installation instructions.
We tested installing ACB and OBM applications on Windows 7, Windows XP, Server 2008, Server 2003, Ubuntu and Mac OS X. Client side applications were easy to install and setup with the given instructions.

The only snag we ran into was the Mac client was unusable. The download and installation worked fine, but we were unable to successfully setup and start a backup process. The client application said the backup completed with errors. After multiple attempts, we were unable to complete a full backup. We did some research on forum posts from multiple websites and tried some of the fixes, but nothing worked in our tests. It seems that other people have had similar issues. The web portal worked and a backup was able to be performed by logging in and manually starting a backup there.

![Backup Progress](image)

Here is an image of the type of problem using the Mac application. Note that the upload was 100% completed while there were 0 files uploaded.

**File Type Testing**

Backups and restorations were performed using the following file types: docx, doc, pdf, vsd, txt, ppt, xls, jpg, png, avi, mp3, html, sql, mkv, as well as Windows System Image and System State backups. All file types were able to be restored and opened on the host computer. Ahsay can restore single files or all files from any backup point. Restoration can be done to the original file location, which will overwrite existing copies or to an alternate location for comparison. Files were restored using both the online restoration from the backup server as well as restored files from local copies.
This image shows some of the file types in one folder that were used in the testing process. Customers select to show all files or just files from a particular job at the top of the screen. Restoration location is selected in the bottom of the screen.

Compression and performance depend on file types. All backups are compressed before they are encrypted and transferred to the backup location. Already compressed file types such as large quantities of jpg or avi files will not compress further and require more processing power and bandwidth to backup than other file types. We saw compression rates vary between 3-57% depending on the file types.

**Browser Compatibility**
The web portal was tested on Internet Explorer, Mozilla Firefox, Google Chrome, and Safari. We tested both the administrator and client sides of the web portal. There were no issues relating to any of the web browsers used. Here are a few screenshots taken with some of the different web browsers.
The only thing that didn’t perform perfectly every time was the restore button on the web browser. Clicking the restore button uses Java to launch a web applet that is identical to the restore application of the OBM or ACB clients. When the applet was closed, clicking the button again wouldn’t always launch the applet again. Closing the web browser and reopening it seemed to fix this problem. This was done on multiple browsers with the same result.

Above is the restore applet launched after clicking on the restore button from the website.

**Database testing**

MySQL was chosen because of its popularity and price advantages. MySQL was installed and a sample database for testing was found on the internet. The test database had almost 4000 lines of
code and over 3500 entries. Although it did save time from having to create our own database, there were about 10 Syntax errors in the code that we had to find and correct. Extra time was also spent formatting and breaking the code into sections which was very helpful in finding the syntax errors. MySQL commands are slightly different than the Oracle DB work learned from class so we also spent a little time researching the commands we were going to need for the test.

The code was edited and saved in notepad as a .txt file before entering it into MySQL.

Preliminary setup included creating a MySQL backup set with the working path to the mysqldump.exe file and a valid database user with appropriate rights and privileges.
The backup set included everything except for the "Information_schema" as instructed in the user manuals.

The backup was run and then I dropped one of the tables.
A restoration was run, restoring the earlier .sql file.

I used "SOURCE C:\Users\Administrator\MySQL\backuptest.sql;" to restore the file to the database and then confirmed that the table and all of the records were restored.

Mail Server

We wanted to test Ahsay's ability to backup an exchange server, but neither of us had one running on our personal computers to backup. We didn't want to interfere with the Ranch's production server and the amount of setup and configuration for a test was deemed to be too much work and hassle. The Ranch suggested skipping the exchange server testing for now. One of Ahsay's main marketing points is their support for backing up exchange servers as a whole or at “brick level.” Ahsay has the option for backing up individual mailboxes so you can handle restorations of a single account rather than having to interfere with every account when restoring. We feel that there wouldn't be issues with the Exchange functionality. There are detailed instructions in the User and Administrator guides as well as demos on performing
exchange backup and restorations on the Ahsay website to see what this would look like and how it operates.

**Functional testing**

**Backup Schedules**

Ahsay supports backing up changes within a file (in file delta.) It uses a data block matching algorithm to track changes. Every backup produces a checksum file in addition to the backed file that is downloaded and used to compare the data blocks between the two files during subsequent backups. Changes are saved to a delta file which is uploaded along with a new checksum file.

![In-file delta technology](image)

The delta type can be set to incremental or differential, with options to upload full files when reaching a max number of Deltas or exceeding a Delta Ratio. The incremental delta will detect and save changes since the last backup while a differential delta will detect and save all changes made since the last full backup every time. Differential deltas limit restorations to just the last full file backup and the desired differential delta file, which is faster, easier to restore, and less susceptible to data loss due to a missing delta file. The downside is that differential backups are larger files which will adversely affect the CPU and bandwidth requirements of each backup, as well as the storage requirements on the server side.

Ahsay also provides a lot of flexibility in setting up backup schedules. Users can set up Daily, Weekly, Monthly or Custom schedules, such as once per year. Users can also schedule any combination of backups they choose to implement both delta types. For example, a user could schedule a full backup once a month, differential backups weekly, and daily incremental backups simply by adding each separate schedule to the desired backup. Various backup schedules were set for different backups, all of which worked without any issues. Backup logs were created and available on the dashboard of the client application as well as the web interface.
You can see all of the backup schedules under the settings for each backup set (above). It was very easy to change the properties of a backup schedule and add multiple schedules to one set. If you want to employ combinations of backup types and schedules, you simply create one backup set of each type and then set up the schedules for those types. Incremental types will automatically see and start from the latest full backups.

There are also two time options for backup schedules. First, you can pick a specific time that you would like the backup to begin like if you would like it to run after business hours or at a designated hour each time. Second, there is also a time interval option. You can set backups to run on set intervals, such as every four hours, or every 30 minutes. If the intervals are spaced too close together, depending on the size and computer resources, the backups might overlap which will cause the later backup to fail and show an error for a missed backup.

Another schedule option is CDP, Continuous Data Protection. Ahsay can be set up to continually protect your data keeping your backups as up-to-date as possible. There are additional advanced options for what to include or exclude under CDP. Since this option will use
more system resources, it could negatively impact the client computer in a significant way. If the user selects the advanced options for CDP, backup controls can be selected to minimize CPU and network traffic by limiting when CDP can or can't be used. CDP is only available with AhsayOBM.

The last type of backup option is the off-line backup. If a computer misses a scheduled backup because it was offline, the backup can either be set to run automatically the when the computer starts or to just give you a reminder that it was missed. We tested multiple backups with multiple schedules and never saw any errors or problems. The highest number tested was an OBM that had 4 different backup sets with two of those having more than one backup schedule setup.

Types of Backups
We wanted to test a few different types of backups to see how Ahsay would handle each scenario. We decided on three different backup set types: backup with small file numbers but large file sizes, backup of large file numbers and small file sizes, backup consisting of a combination of both. For the first test, I used large .iso images that were 6-7 GB each. For the second test, I gathered a few thousand small text, video and image files. For the third test, I used a combination of a few large video files around 1GB each and numerous Microsoft Office files.

Each test was backed up and restored. Files were randomly selected and opened to ensure complete restoration without data loss or corruption. Every test was successful. Ahsay seems to handle fewer large files faster than thousands of small files. That is to be somewhat expected, since it takes longer to spool up and process, compress, and encrypt multiple files rather than one even if the overall size is the same.

One last test was performed on full vs. incremental backups. Whether doing an incremental or full backup, time and performance depended most on the size of the backup file. An incremental file that was 500Mb only took slightly longer than a new 500MB backup. The increased time is probably due to comparing and creating a delta file.

Bare Metal Backups
A bare metal backup was tested using a test computer setup with Microsoft Server 2008 R2 Enterprise edition 64-bit OS. Ahsay uses the Microsoft backup software to create the full and incremental backup files. Unlike the previous versions of Microsoft Server, 2008 uses new backup program that has to be added as a server feature, instead of being included by default. The program also uses a new file structure of .vhd instead of .bku. Ahsay basically just runs a Microsoft backup, and then just handles the compression, encryption, and storage of that file for
the user. Restoration then involves downloading, decrypting, and decompressing the files for you to perform your own restoration using the Windows backup software.

Bare metal backups were performed and restored without incident. The process was done both using the Seed Load Utility with external media and over the web. Some minor bumps in the road were encountered, but that was due mainly to settings and Microsoft’s new guidelines for Windows Server Backup. Microsoft requires you to have a separate drive larger than the one you are backing up. The drive also has to be formatted in NTFS. Backups are now at the block level of the HDD, so you can only select which drives are to be backed up.

The first problem was that with the seed utility, we had the backup set to use the external media drive for temporary spool location of the backup. During the subsequent tests using the network connection, the backup wouldn’t work because the external drive disconnected and couldn’t find the temporary spooling location.

Another issue is that we wanted to test doing a cold site disaster recovery trying to restore a backup of one server from a HP desktop computer to an IBM laptop. Both were running Microsoft Server 2008 R2 Enterprise edition 64-bit OS. During the restore process, there was a Windows error displayed that the backup belonged to a different computer and this wasn’t supported by Windows. The file would restore but go into a boot error loop stating hardware changes were the culprit. After testing this about 7 different ways including performing new backups and restoring them without Ahsay. It was clear this is a Windows issue and not due to Ahsay. It was found that Server 2008 only supports restorations to the same hardware.

As long as it was the same hardware, the backup restorations worked without any problems. We did one last test representing a hard drive failure. The backup file was restored to an external media drive using a different OBM client. The internal Sata HDD was then swapped out for a new HDD and the Server 2008 installation disks were used to recover the computer using the external file. With the new .vhd files, the restoration includes the drive letters and sizes from the backup. Our test went from a 80GB HDD to a 1TB drive, the restoration formatted the new drive with a 80GB section identical to the original, leaving the rest as unallocated space. Note that you also have to restore to a drive the same size or larger. We were obviously unable to take screenshots from computers during the restoration, including the errors given.

Backup Limits
Storage limits and available features are set by the administrator when the accounts are created. The storage size can later be scaled up or down by the administrator at any time by simply changing one number and clicking the update button. Features (database support, delta merging, exchange support, etc.) are simple check boxes that can be turned off and on just as easily. The storage space consists of two areas for each user: the data area and retention area. The data area contains the current backups in storage for the user and the retention area contains deleted backups. Retention settings chosen by the user will determine how long a deleted backup is kept on the system before permanent removal. The default is 7 days.
When the user is approaching the backup limit, the system can be set to send an email to the account contact notifying them of the pending issue. Options to the user include contacting the administrator to increase the storage size, or removing older backups by deleting and managing the retention area. Users can backup until they reach the backup quota on the backup server and then the current backup will fail with a Quota Exceeded error.
Once the quota size is exceeded, all backups will fail to start until the problem is fixed by one of the methods mentioned above. Removing older backups or adjusting the size both fixed the problem without errors.

Ahsay can also be set to allow trial accounts without administrator permission. When enabled, trial accounts are customized with a predetermined quota size, feature set, and expiration policy. Users only require the address of the AhsayOBS server to install and sign up for a trial account. Trial users do not count towards the maximum number of users allowed within AhsayOBS by the software license and there can be unlimited number of trial users within AhsayOBS. However, each backup user can have a maximum backup quota of 100GB for a trial period of 30 days. After expiration of the trial period, the backup quota will reset to a maximum of 500MB automatically.

**Admin Controls**

The administrator can control every aspect of the backup service through the web site. Some of the controls include suspend, adjust quota size, set user restrictions like bandwidth controls, change feature options, change backup schedules, change backup sets, and enter new user login passwords.

Other Admin controls include the ability to manage group policies for users, set up and change server configurations like SMTP settings, set in file delta settings that apply to all Ahsay ACB users, and setup and manage advertisements that can display on all Ahsay client applications. Besides testing the quota size adjustments shown earlier, we decided to test manually firing a backup on the client computer as an administrator and also suspending an account.

Selecting a backup set and firing it manually from the Admin account in the web portal test:

1. Selected one backup set and clicked the Run Backup button at the bottom of the screen.

The "Backup is Pending" column will change from “No” to “Yes.”
2. The AhsayOBM application on the server machine owning that backup service used pop up balloons to show when the application was starting and stopping the backup process.

3. The backup fired and completed. The last backup date in the browser and on the client side dashboard both updated to reflect the new backup performed. The administrator account also has the ability to cancel a backup on this same screen or to even delete backup sets under the user account controls.

Suspending and account test: A suspended account will not allow any further backups and give a “Suspended account” error to the user instructing them to contact the administrator. While doing another backup, the user status was changed from Enable to Suspend which resulted in the backup halting and giving a permission update error due to UserSuspendedExpt.

**Backup Interruptions**

We came up with a list of backup interruptions that we wanted to test to know how the software will handle different real world scenarios that will most likely happen sooner or later. We decided on offline clients, client side computer crashes, down network connection, server side crashes, and an offline server during a regularly scheduled backup.
We simply powered down the computer during the scheduled time for an offline test. The server recognized the missing backup and tried to send an email report to the client about the missed backup. The email settings can be turned on or off on the admin site. This also happened to be the same result we saw when the backup server was offline during the scheduled backup. When the server comes back on, the program reports all scheduled backups missed during the downtime. Note that this is not an error and was not seen in the error reports for the admin.

We restarted the client computer to represent a client computer crash during a backup. The backup fails at that point and a “Backup not finished” error is created and shown on the server logs and client application. The backup is not restarted by the software and will remain like that until the next scheduled backup.

The next test was a network connection failure. We simply disabled the network device, thus severing the connection. The backup software simply waited for a connection to re-establish and continued the backup where it left off. This was the exact same result found for the backup server crash done by rebooting and also stopping the backup service. Time intervals for how long the backup would wait and keep trying included 2, 8, 15, and 40 minutes. The Ranch has a zero down time for their services and many levels of redundancy so I figure this was sufficient for their BCP plans.

**Seed Loading**

To reduce time and bandwidth requirements for large initial backups, Ahsay supports a Seed Load backup option. The backup is performed and stored onto a removable media that can be shipped and uploaded to the server storage instead of transferred over the internet. This avoids the internet bandwidth bottleneck, greatly reducing the time and resources required on both the server and client sides. The data is compressed and encrypted before being stored on the external storage source and, as always, doesn't include or ship with the encryption key so the risk of loss in transportation is minimal. Once the media arrives on site, it is simply a matter of copying the file folder to the file folder within the user’s storage location. Once there, the data is available for future delta backups and all restoration options. The process can be reversed just as easily requiring a computer with a AhsayOBM installation and the encryption key on the client side to decrypt and decompress the files before restoration is possible.
As with a regular file restoration, the restore can be performed to the original or alternate destinations as well as be used to restore the files to a completely different computer. To perform a seed load copy, the user can select this option under the options button when performing a backup operation.

Windows bare metal backup and system states were performed using the Seed Load Utility to an external hard drive using a USB 2.0 connection. The files were then transferred to the backup server and transferred to the client’s storage space. Once there, file verification has to be run by the administrator on the client’s account. This will update the backup information and storage on the web portal and also on the client side application the next time it is refreshed. Once the backup was shown on the backup server, incremental backups were tested and run successfully. After the incremental backups, the process was reversed and external media was used to transfer and restore the backup on the computer. All tests ran perfectly with no errors.

Local copy is another option for users to retain a complete copy of the backup on-site. It will be compressed and encrypted the same as the copy sent to the backup server. Backups and restorations using a local copy will be faster since the internet transfer backup is usually the largest performance bottleneck. The advantages of maintaining a local copy over a one-time seed load copy is that the in-file delta backups, backup schedules, and retention policies can all be applied to the local copy, just like they are to the online backup copy on the server. AhsayOBM and the encryption key will be required to use or restore a local copy.
Restorations
All restorations using Ahsay were done successfully. Some of the details about restored file types and restorations done using Seed Load Utility and Local Copy have already been covered earlier. 1000’s of files have been restored to both the original and alternate locations without fail. There was no instance of data loss or corruption during any of our tests.

There was one false alarm from a restoration error involving a .ppt file to mention. One of the backup’s server logs showed an error on the web that wasn’t on the Client logs. The error listed the file and said that one of the block file sizes was different than what it was expecting.
The file in question was restored to an alternate location and compared to the original with no apparent issues. The restored file opened and functioned normally. This wasn't a real issue but any time the software outputs a false positive it can make the clients nervous about the backup and product in general.
Security

Each backup account is protected with a login name and password used for the client side application and the web console. When logging into AhsayOBM or AhsayACB, you enter the address of the AhsayOBS server you will be connecting to and select whether to use http or https which supports 128-bit SSL channel support. The connection type is located in the options area of the login screen on the client application. If the user chooses to save their password, the connection will be saved as well for each login.

Every Backup set is required to select an encryption level when it is created. If the user keeps the default settings, Ahsay will use a 256-bit AES Encryption algorithm with an ECB encryption mode using the login password as the encryption key. The user can also set up a custom encryption setting, using 128 or 256 bit key lengths; ECB or CBC encryption modes; a custom encryption key; and the choice between Twofish, Triple DES, or AES algorithms.

All backup data is compressed and encrypted before it is sent to and stored on the AhsayOBS server. The key is never sent to the storage server and the client is responsible for remembering the encryption keys. All data sets will be unrecoverable without the encryption keys used. If the client's password is changed, all default encryptions from then onward will use the new password and the old password will be required to decrypt all previous backups using that password. User
passwords are only shown to the admin in a hashed format. If clients install AhsayOBM on a different computer, they will be asked for the encryption key to all of the backup sets in order to decrypt and restore those backups.

Online restoration can also be restricted to certain IP addresses if the client desires the extra protection. This would prevent any attempts to restore the backup files to another computer even if the account is hacked with a valid password. User accounts can also be set to lock after 3 failed login attempts to prevent people or computers from trying to crack unknown passwords.

Some backups require use of a temporary directory to store files while performing the backup. Once the backups are completed, the temporary files are deleted. During the process of one of the backups, I went to the temporary directory to see how the backup files were being stored in that directory. The files were compressed into folders named with a string of numbers and there were no discernible file types that could be read within the folders. Here is an image below. Note that Ahsay does state that some backups like a Windows System state or some database backups will use a temporary file to store the unencrypted files. This is necessary to build the backups or shadow copies before the files can be compressed and encrypted. All temporary files were removed from the test computers once they were no longer needed without trace of using the recycle bin.

![Temporary Directory Files](image)

**Performance**

Bandwidth and time performance have a great deal of variation due to the files being transferred, bandwidth restrictions of user accounts or ISP connections, computer resources to build and send files, hard drive read/write capabilities, etc.

The first backup I tested with the Ranch computer was a backup set consisting of many small files, totaling 5.84 GB of data. It took 18 hr 13 sec with a transfer speed of 750.70kb/s. The backup was created fairly fast, but the Upload ran slowly. We ran a connection test on speedtest.net and saw the connection was only getting about 1Mb/s down and up. We contacted
the Ranch and asked them if there were any bandwidth restrictions and they told us the servers were throttled down to 1Mb/s. The servers were plugged into their DMZ on their company T1 connection. Testing could have slowed the network down too much, impacting their business. It is pretty hard to test performance when we have such a large bottleneck with the internet connection.

To get around this, we set up a secondary test site at home. The server specifications were as follows: Windows 7 Professional SP 1 64-bit OS, 8 GB Ram, Intel Core i5 760 (2.8GHz Quad core,) and a Xfinity 12Mb/s connection speed tested at 16 Mb/s carried over a Wireless G network. Test computers consisted of a HP Desktop with an Intel Pentium 4 HT 2.8 GHz computer and 3 GB of RAM, and a IBM laptop with a Intel Dual Core 1.8 GHz processor and 4 GB of RAM. Both test computers were imaged multiple times with multiple OS’ during the testing procedures.

The new setup had speeds of 17 Mb/s over the wireless G network and saw backup performance of 3 Mb/s from an additional test computer from South Jordan that had similar specs to the server test computer. Here is a backup that took 1 hr 21 min to complete a 11.9G file upload to the backup server over on the same wireless network.
It is important to know that Ahsay is performance-oriented with some of their options like the Seed Load Utility and Local Copy. Two backup sets that were done as a seed load utility onto an external hard drive using a USB 2.0 connection had much faster times. It took 28 min for an 8.15 G backup and 20 min for a 11.0G backup. Both finished with a respectable transfer rate of over 40Mbit/s. Most incremental backups are going to be fairly small after the initial full backups. Seed loading will bypass network bottlenecks altogether.

There are other performance settings that are going to have a large impact for your overall server. Backup schedules can be manipulated to spread out the clients schedule so they aren’t all trying to upload at once. Options like CDP can be disabled. Delta merge can also be turned off if necessary. Delta Merge is a service that once a restoration is chosen, the server will combine full and incremental backups up to that point and merge them into a single file for transfer and restoration. While this is a very nice option, it is going to negatively affect the server side computer resources.
Lastly, you can also control bandwidth on individual user accounts. If you have one super user that wants to run full backups throughout the day, you can restrict that user's bandwidth in Bits/Second intervals on the admin site. This can more appropriately shift a performance bottleneck from the computer or internet connection to the user that requires it.

Management
To aid with monitoring and managing numerous backup clients and accounts, Ahsay offers different User and System Reporting options that are emailed to the email addresses on file. User reports include backup, online restoration, setting changes, missed backups, inactive user periods (defined by admin,) Off-line Backup reminder and backup quota reminders (default is set to warn users when they approach 90% of their storage quota.) System reports such as usage, error and replication errors can be configured to automatically email the information to the administrator when detected. Certain system jobs can also be set to fire automatically or wait until the administrator manually performs the tasks, such as applying retention policies or removing inactive users. The image below shows how easy it is to change these admin helper features.
Besides the reports, the admin account also has access to review logs such as the system, backup, restored, backup error, replication, and advertisement logs which are sorted to date under the manage log tab in the admin account. Here is an example of an error log from 3-10-12 with included information below.

The admin and users can also access backup reports and storage statistics through the web portal or client side application dashboards. Recent backups can quickly be reviewed to see errors and identify backup issues.
Customization and Branding

The Ahsay Customization Portal (http://partners.ahsay.com/) allows you to do the followings:

1. Building custom installers for the followings Ahsay products:
   i. AhsayOBS and AhsayRPS
   ii. AhsayACB and AhsayOBM
   iii. AhsayNCU (For AhsayOBS v5.5 or below)
2. Set the vendor name, support email, and URL to your own values;
3. Put your own company logo and other images into the software;
4. Set the default backup server hostname, TCP port number, and protocol (HTTP/HTTPS) to your own values;
5. Hide/Show encrypting key checkbox in AhsayACB/AhsayOBM;
6. Hide/Show language selection list in AhsayACB/AhsayOBM;
7. Hide/Show the backup server URL textbox;
8. Set the default language for AhsayACB/AhsayOBM;
9. Enable/Disable languages for AhsayACB/AhsayOBM;
10. Enable/Disable user account profile update from AhsayACB/AhsayOBM; and
11. Customize the terms of use statements shown in the installer of AhsayACB/AhsayOBM.

Once you have made all the customization you want, you can download a customized version of AhsayOBS / AhsayACB / AhsayOBM / AhsayNCU from the download page (shown below) of the customization portal.

Only purchased licenses are able to login and access the customization portal, so the trial version is unable to be fully customized. Customization should be performed before installation of other Ahsay applications. Once finished, the customization portal allows you to download a customized and fully branded AhsayOBS which includes the download of the fully customized AhsayOBM and AhsayACB client applications. The available download is only available for 24 hours from the customization portal so you will need to set aside enough time to finish, or you will have to start over.
Above is an example of what a customized Client side application could look like after customization.

**Pricing**

The software is priced based on the number of Client Access Licenses (CALs) from the client side applications (AhsayOBM and Ahsay ACB), Brick level exchange mailboxes, and number of virtual machine licenses. The server side software (AhsayOBS and Ahsay RPS) are free, and there is no start-up or branding fee required. The software can be purchased or leased for a per license fee with increasing price breaks depending on the number of licenses. There is also a support and maintenance fee per license per year after purchasing (starting one year after activation) which covers support and future upgrades. The current prices are listed in the graph below.

### Table 1 - Pricing of Purchase Package

<table>
<thead>
<tr>
<th>No. of Client-Side Backup License</th>
<th>AhsayOBM (USD)</th>
<th>AhsayACB (USD)</th>
<th>Brick-Level Exchange Mailbox (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$120</td>
<td>$10</td>
<td>$10</td>
</tr>
<tr>
<td>2</td>
<td>$200</td>
<td>$20</td>
<td>$20</td>
</tr>
<tr>
<td>3</td>
<td>$300</td>
<td>$30</td>
<td>$30</td>
</tr>
<tr>
<td>4</td>
<td>$360</td>
<td>$40</td>
<td>$40</td>
</tr>
<tr>
<td>5</td>
<td>$460</td>
<td>$50</td>
<td>$50</td>
</tr>
<tr>
<td>10</td>
<td>$1,750</td>
<td>$150</td>
<td>$150</td>
</tr>
<tr>
<td>200</td>
<td>$12,000</td>
<td>$1,200</td>
<td>$1,200</td>
</tr>
<tr>
<td>300</td>
<td>$10,000</td>
<td>$1,000</td>
<td>$1,000</td>
</tr>
<tr>
<td>400</td>
<td>$12,000</td>
<td>$1,100</td>
<td>$1,100</td>
</tr>
<tr>
<td>500</td>
<td>$25,000</td>
<td>$1,500</td>
<td>$1,500</td>
</tr>
<tr>
<td>600</td>
<td>$35,000</td>
<td>$2,000</td>
<td>$2,000</td>
</tr>
<tr>
<td>1,000</td>
<td>$40,000</td>
<td>$20,000</td>
<td>$20,000</td>
</tr>
<tr>
<td>2,000</td>
<td>$45,000</td>
<td>$25,000</td>
<td>$25,000</td>
</tr>
</tbody>
</table>

Contact our sales representative for further details.

**Add-on modules included:**

- In-File Delta
- Volume Shadow Copy
- Server Replication
- Exchange
- SQL
- Oracle
- Domino/Notes
- MySQL

**Standard Support & Maintenance Fee:**

- $12/CAL/Year
- $7/CAL/Year
- $0.75/Mapbox/Year

*Competitive Upgrade is available, please refer to notes below.

*Yearly Standard Support & Maintenance Fee includes software upgrade (FREE for the first 12 months)
CAL = The number of backup accounts created on the backup server.

Exchange Mailbox License = total number of mailboxes created on the backup server.

<table>
<thead>
<tr>
<th>No. of Guest Virtual Machine Licenses</th>
<th>AhsayOBM price per license</th>
<th>AhsayACB price per license</th>
<th>Brick level Mailbox prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>$120</td>
<td>$60</td>
<td>$10</td>
</tr>
<tr>
<td>25</td>
<td>$110</td>
<td>$55</td>
<td>$10</td>
</tr>
<tr>
<td>50</td>
<td>$100</td>
<td>$50</td>
<td>$10</td>
</tr>
<tr>
<td>250</td>
<td>$90</td>
<td>$45</td>
<td>$10</td>
</tr>
<tr>
<td>500</td>
<td>$80</td>
<td>$40</td>
<td>$10</td>
</tr>
<tr>
<td>500</td>
<td>$75</td>
<td>$40</td>
<td>$10</td>
</tr>
<tr>
<td>100</td>
<td>$70</td>
<td>$35</td>
<td>$8</td>
</tr>
</tbody>
</table>

Given the pricing structure, we recommend that you purchase licenses in blocks of 5 at a time. This gives the optimal price break without incurring too many licenses that would either expire, or result in large overhead costs. CALs purchased can be put on stock until the end of the following year. Brick level mailbox licenses should only be purchased at the clients request and for the exact number specified since there is no pricing incentives to buy extras. Brick level Mailboxes are also a luxury item since the entire exchange server can be backed up at no additional cost with the basic Ahsay OBM license. VM price breaks come in large intervals and only offer $5 difference per level so they should be purchased in the minimum number allowed and only as needed. One AhsayOBM license can also be used to backup multiple computers if it is set up correctly with the appropriate access and permission levels.
The lease option is cheaper to start, but way more expensive and less profitable in the long run. Even at the most expensive level of purchasing an individual license, it would take less than two years to break even between the purchase and lease costs while ongoing maintenance fees for a purchased license would be 1/6 of the cost ($12 vs. $72) of leasing annually. The breakeven point is even sooner if purchasing multiple licenses at the same time.

Two optional additional fees (depending on NAS usage and OS selection) are:

- **Recommended specs for optimal performance**

  AhsayOBS should be installed on a machine supporting 64 bit multiple CPU and multiple cores. A 64 bit Operating System will allow AhsayOBS to run on a 64 bit Java JRE platform, as 64 bit Java is capable of supporting larger Java heap size settings. This type of configuration will provide sufficient capacity for future business expansion, to meet the needs of existing customers, and to support new AhsayOBS server features.

  AhsayOBM is recommended to be installed on a 64 bit machine, with multiple CPUs and cores, especially for environment setup, with application specific backup module, such as virtual machine, MS Exchange, or bare-metal backup.

  AhsayOBM/AhsayACB v6 clients are enhanced to utilize multiple threads for backup and restoration. It is recommended to keep this number to around 300 user accounts, to avoid potential performance problems.

  Due to features such as CRC checking, delta merging, and support for image, Hyper-V, VMware backup sets AhsayOBS v6 may require more Java memory, although there is no exact formula for calculating the correct Java heap size setting for any given AhsayOBS server. In general a maximum Java heap size setting of at least 2048M is recommended, assuming AhsayOBS is running on a 64 bit Operating System.

  When setting the maximum Java heap size for AhsayOBS please ensure this value does not exceed 50% of the RAM on the server, to allow sufficient memory for O/S processes and operations.

  Minimum Specifications are as follows:
The following is the Requirements for AhsayOBS / AhsayRPS / AhsayRDR / AhsayOBM / AhsayACB:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>AhsayOBS / AhsayRPS / AhsayRDR</th>
<th>AhsayOBM / AhsayACB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Dual Core architecture or above</td>
<td>CPU</td>
</tr>
<tr>
<td></td>
<td>N/A  60%</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>Minimum: 1 GB Recommended: 2 GB or above</td>
<td>Memory: Minimum: 512 MB Recommended: 1 GB or above</td>
</tr>
<tr>
<td>Disk space</td>
<td>Minimum: 566 MB required for program installation</td>
<td>Disk space: Minimum: 300 MB required for program installation</td>
</tr>
<tr>
<td>Java Version</td>
<td>Minimum: Java 1.6x23 or above</td>
<td>Java Version: Minimum: Java 1.6x23 or above</td>
</tr>
</tbody>
</table>

* Multiple thread support is available for backup and restore, including Local Copy, Seed Load, and Decrypt functions.

Given the current hardware options and pricing, we recommend using at least a 2.5Ghz Quad Core CPU with 16-32GB of RAM. This is around the current “sweet spot” for price/performance and this would allow for some future proofing, good performance, and be economical as well.

**Conclusions/Reporting to the Ranch**

We encountered a couple of hang-ups during the project that we feel we should mention. First was we were not able to test an Exchange instance as we had planned because it would have been too hard for the Ranch to allow us access to back up their Exchange service. Second, we discussed getting a test database from the Ranch but never followed up with them about it. What we did once we realized that we hadn’t followed up with them was we pulled a sample database and changed the syntax to be able to get it to work with MySQL. Third, Ahsay branding is not available unless a license is purchased. We notified the Ranch this was the case and they were ok with the fact that we did not test this portion for Ahsay. Last and probably our biggest hang-up was the fact that we were doing our backups over a T1 connection. This limited the speed greatly and caused backups to take a large amount of time. This could have also contributed to some of the backup failures we encountered.

Syncrify is a very inexpensive product. It is the most inexpensive product that we found. The cost of Syncrify might play into the reasons for its very limited feature set. We believe that Syncrify is in its infancy as a product. Possibly in the future it will have a better feature set like most of the other products in the market. Syncrify as an application does not have the ability to distinguish different services that it is backing up (e.g. Exchange, web server, etc.) It is a single file backup service. It treats every file the same.

The administration features in Syncrify are very minimal. The admin features are lacking during a backup process and as a feature set in general. Other than pausing or restarting the entire Syncrify service, no other admin features are available during a live backup. Also, as noted above, Syncrify had difficulty backing up large files. Based on that alone, we would not recommend the Ranch to offer this product to their clients. The branding features in Syncrify were also very limited and did not work as advertised. However, we did mention to the Ranch because of its price Syncrify might work as an in-house backup solution. It is much cheaper to purchase licenses, and because the product will not be offered to customers, there is minimal risk to using it in-house.
Ahsay is a good fit for the Ranch to start their Online Backup MSP. We feel that Ahsay meets all of the requirements and meets the affordability/profitability level that the Ranch needed. Ahsay is a full-feature product that will cover any business needs of the small to medium target customers as well as large businesses, if the opportunity arises. Ahsay is a product that can start small, and easily scale up quickly and inexpensively with very little capital or risk. The performance and reliability that we saw during testing will help maintain the Digital Ranch's reputation that they have established over the last decade.

The administrator controls are extensive and can be accessed from anywhere there is an internet connection for remote management. Ahsay's monitoring and reporting allow the Ranch to quickly and easily see the system health and performance. The ease of use will help reduce the number of hours and consultations required to setup and maintain the service so that the Ranch can offer this service without having drastic changes to their expenses or workload. Ahsay has been very successful focusing only their partner relationships and expanding product offerings and compatibility as technology advances making it a product you can trust will be there in the future.

As part of the software selection process, we prepared a report for each application for the Ranch. We took about a week to prepare everything and make recommendations before presenting our findings to the Ranch. Most of the separate reports were used in the creating of this report. Upon reporting our findings to the Ranch for each application, they seemed happy with what we reported. As part of our presentation, we answered all of their questions and offered our services during the installation/implementation of Ahsay. At the timing of our reporting to them they were not ready to install Ahsay and start the offering it to their clients. We also left open the channel of communication for if they had any questions in the future about Ahsay. We also promised a prompt response, as we have cleared up the communication problem we were having previously in the project.

**Key Takeaways**

Throughout the project’s life cycle, we ran into a couple of issues. Every issue we had could have been resolved with communication. At one point during the project, we thought the Ranch had told us to wait and we would hear back from them on the progress of the project. They then contacted us sometime later and asked how the progress of the project was coming. It turned out they either didn’t remember saying to hold on the project or they didn’t say it at all. This small issue could have been resolved easily had we just communicated up front with the Ranch. Also, there were times throughout the project where it would take a couple of days for us to respond to an email. Before we responded to an email, we wanted to talk about the response we wanted to give the Ranch. Our schedules were very different; Jacob works at night and takes care of his daughter during the day, Zach works during the day and travels for work a lot. If we were to do our project over again we would put together a communication plan that would be better for us and the Ranch.

The project we did was real-world experience. Jacob has been a part of similar projects at his current job. Zach is in the process of selecting an ERP system for a contracted company and will use some of the skills he learned during this project to help. Many companies are either looking for a new way to boost revenue by offering a service, or by upgrading or changing a current software platform. For this project we went through the full process of researching a market, researching multiple products, selecting products to test based on agreed upon criteria, testing the products functionality, and selecting a product that best fits the Ranch’s needs.
For this project we used skills and techniques we acquired in the MSIS program. First and foremost were our project management skills. We planned out our project before we got started based upon taking the project management class. However, we also learned that our project management skills still need to be refined. We also used skills we learned in the systems analysis and design class to create the multiple different matrices used to create the software selection criteria. We used skills we learned in the network defense class and security class to set up the different network when we were testing Ahsay. We learned how to use Wireshark in the security class and tried to capture packets during a live backup. We changed and updated a MySQL database with skills we learned in the database class. Overall this project was a good learning experience for us and a lot of fun. Although we are glad that we are finished with it!

**Works Cited**


<table>
<thead>
<tr>
<th>Page 3: [1] Formatted</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [2] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [3] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [4] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [5] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [6] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [7] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [8] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [9] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [10] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [12] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
<tr>
<td>Page 3: [13] Formatted</td>
<td>Author</td>
</tr>
<tr>
<td>Default Paragraph Font, Check spelling and grammar</td>
<td></td>
</tr>
</tbody>
</table>