
UNITRENDS VAULT2CLOUD™ AND PRIVATE VAULTING FREQUENTLY ASKED QUESTIONS

CONTENTS

Preface	1
General Questions	1
Vault2Cloud™	5
Protecting Data	8
Management and Monitoring	11
Recovering From An Event	13
Recovering from a Disaster (Replacing the On-Premise Appliance)	14
Scaling and Provisioning	15
Licensing	23
VSP: Vaulting Service Provider Using Private Vaulting	24
Future Direction Questions for Private Vaulting	26
Miscellaneous	27

PREFACE

Unitrends offers two fundamental types of vaulting: Vault2Cloud™ and private vaulting. Many of the questions and answers in this document refer to both; however, when there is a difference that difference is explicitly called out as being specific to Vault2Cloud™ or private vaulting.

GENERAL QUESTIONS

1. What is the version of Unitrends software to which this Unitrends vaulting FAQ refers?

This FAQ refers to Release 4.2.2 or later unless the release is specifically called out otherwise.

2. What is vaulting?

Vaulting is the process of electronically sending critical data from a customer's premises to some other location for the purposes of providing disaster recovery.

3. What is disaster recovery?

Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of a customer's technology infrastructure after a natural or human-induced disaster.

4. How does vaulting relate to disaster recovery?

Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of a customer's technology infrastructure after a natural or human-induced disaster. Vaulting is a technique used to achieve disaster recovery through the electronic transfer of data from the customer's premises to some location far enough away to increase the probability of recovery in the case of a wide-spread disaster.

5. What is business continuity?

Business continuity describes the process, policies, and procedures related to how a customer will recover from partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

6. How does disaster recovery relate to business continuity?

Disaster recovery is a subset of business continuity. Business continuity describes the process, policies, and procedures related to how a customer will recover from partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

7. How does vaulting relate to rotational archiving (via either D2D2D or D2D2T)?

Rotational archiving is another mechanism for disaster recovery. D2D2D (Disk-to-Disk-to-Disk) is supported by Unitrends via its SDA (Single Drive Archive) and MDA (Multi-Drive Archive) capabilities. An archive copy of one or more backups is made to one or more disk and these may be rotated off-site. D2D2T (Disk-to-Disk-to-Tape) works basically the same way.

The advantage to using rotational archiving is that it doesn't require the cost of a WAN (Wide Area Network) between the customer's site and the vaulting location. The disadvantage is that it's incredibly prone to human error and it ends up being much more expensive than the price of the WAN due to the actual operating expense of the personnel that have to try to implement the rotational strategy.

Unitrends has many customers that use both – they use vaulting for their most critical data and they use D2D2D archiving for their less critical data. In addition, we have customers that use D2D2D for longer-term archival than is available on the on-premise appliance.

8. What is a DPU?

Unitrends uses the term "DPU" to refer to its on-premise (i.e., on-site) appliance. The acronym stands for "Data Protection Unit." The on-premise appliance is the heart of our business continuity and data protection architecture – a local business continuity appliance that provides local retention and which optimizes the amount of data that needs to be sent off-site for vaulting.

9. What is Vault2Cloud™?

Vault2Cloud is Unitrends cloud-based vaulting solution. It is offered completely as a service; a Unitrends customer who has on-premise protection is able to achieve disaster recovery without purchasing any additional equipment.

10. What is private vaulting?

Private vaulting is when a customer owns all of the equipment required for vaulting. In other words, the customer owns both the on-premise and off-premise appliances.

11. What is a DPV? How is a DPV different from a Vault?

Unitrends uses the term “DPV” to refer to its off-premise (i.e., off-site) appliance. The acronym stands for “Data Protection Vault.” The off-premise appliance is the heart of our disaster recovery architecture – a remote disaster recovery appliance that provides remote disaster recovery.

The terms “off-premise appliance”, “DPV”, and “Vault” are used interchangeably and mean the same thing.

12. If I am using Vault2Cloud, do I have to care what an off-premise appliance is?

No, you don’t have to care. The off-premise appliance is embedded in a cloud-based service.

13. What is D2D2x?

This is an acronym that means Disk-to-Disk-to-Any. It refers to the fact that disaster recovery can be achieved using our on-premise D2D appliance which can then either use rotational archiving via disk (recommended), tape (not recommended), or cloud (recommended.)

14. What is cross-vaulting?

Cross-vaulting is a unique offering that lets companies with just a few remote sites elect to use a single Unitrends appliance per-premise as both an on-premise appliance (for on-premise protection) and an off-premise appliance (for off-premise protection.) Logically, a single appliance is monitored and managed as both an on- and off-premise appliance at the same time.

15. Using cross-vaulting, can I set up at a single location both business continuity and disaster recovery?

No, because to do disaster recovery you need for the off-premise appliance to be located off-premises so that in the event of a man-made or natural disaster the data can be retrieved. Cross-vaulting is useful if a company has two or more geographically separated locations.

16. What is half cross-vaulting?

Half cross-vaulting simply means that a Unitrends appliance is set up as both a on- and off-premise appliance but that the Unitrends appliance is not set up to vault to an off-site appliance (which would be cross-vaulting.) Half cross-vaulting is not a typical configuration because the on-premise appliance behavior of the vault is not protected against disasters while simultaneously the off-premise appliance section is protecting other on-

premise appliances from disasters; however, it is possible to configure a Unitrends appliance as a half cross-vault and use it in that manner.

17. How is a vault different than vaulting?

The vault is the off-premise appliance upon which the protected data is transferred and stored. Vaulting is the process by which that protected data is transferred from the on-premise appliance to the off-premise appliance.

18. Does Unitrends offer data protection without vaulting?

Yes. Data protection simply implies that a customer wants some form of recovery in the case of some type of loss of data. A customer may buy an on-premise appliance without electing to perform any form of disaster recovery – including vaulting. In other words, a customer may buy an on-premise appliance to recover from an interruption of critical function but may gamble that a true disaster won't befall his or her business.

19. Does Unitrends offer business continuity without vaulting?

Yes. Business continuity describes the process, policies, and procedures related to how a customer will recover from partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. A customer may buy an on-premise appliance to recover from an interruption of critical function but may gamble that a true disaster won't befall his or her business.

20. Does Unitrends offer disaster recovery without vaulting?

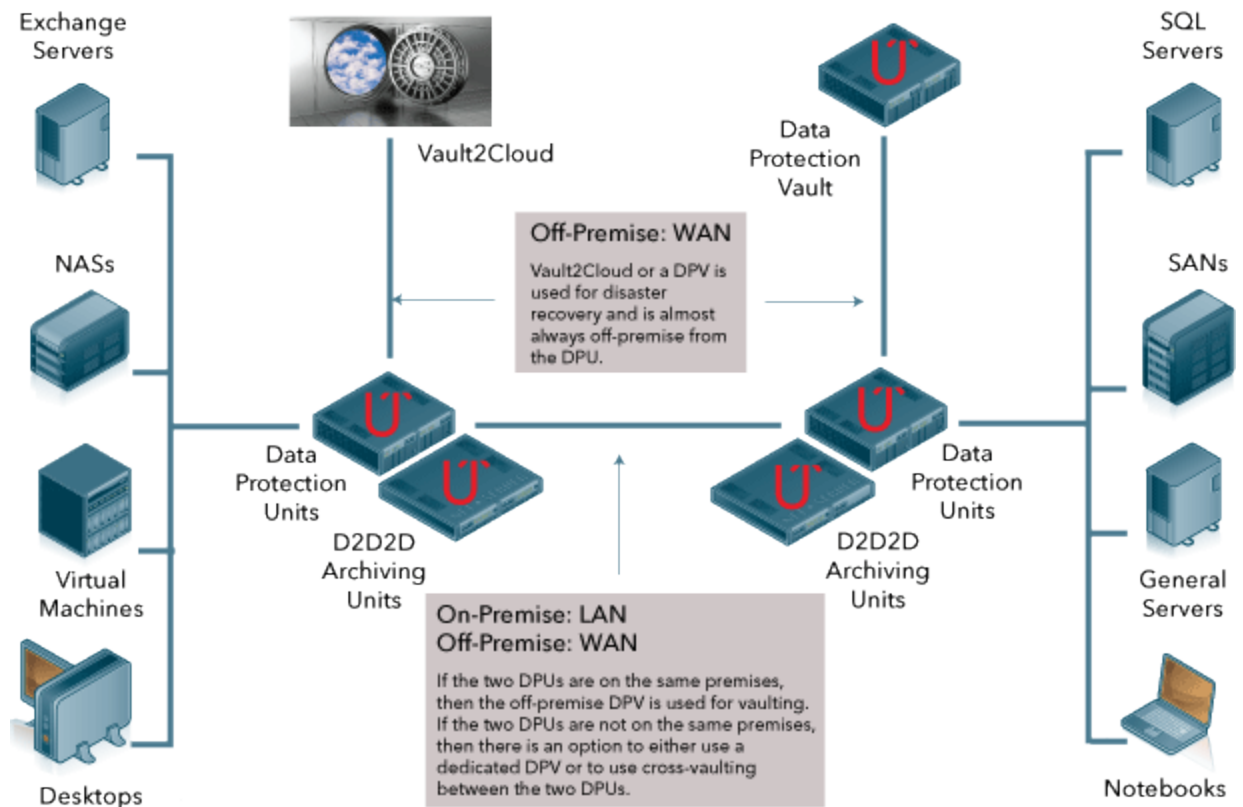
Yes. As mentioned in a previous answer, Unitrends offers rotational archiving via D2D2D and D2D2T archiving.

21. Does Unitrends offer disaster recovery without business continuity?

No. This is what typical SaaS (Software as a Service) backup vendors offer (e.g., Mozy, HP Upline, etc.) Without an on-premise appliance, you can recover from a disaster – but very, very slowly as you wait for gigabytes and terabytes of structured and unstructured data to download over an Internet connection.

22. Can you show me a general high-level diagram of your architecture?

Yes; a diagram showing our high-level architecture that includes private vaulting and Vault2Cloud is depicted as follows.



VAULT2CLOUD™

23. What is Vault2Cloud™?

Vault2Cloud is Unitrends cloud-based vaulting solution. It is offered completely as a service; a Unitrends customer who has on-premise protection is able to achieve disaster recovery without purchasing any additional equipment.

24. What are the primary advantages of Vault2Cloud™ versus private vaulting?

Vault2Cloud allows Unitrends customers to obtain the advantages of private vaulting without the capital expenditure and operational expenditure associated with private vaulting.

25. What are the primary advantages of private vaulting versus Vault2Cloud™?

Private vaulting allows customers who have multiple facilities to take advantage of disaster recovery without recurring fees and to configure their on-premise and off-premise configuration more flexibly.

Private vaulting allows more frequent RapidSeed™ operations to be performed without incurring Vault2Cloud™ RapidSeed™ fees.

Private vaulting allows complete disaster recovery tests and audits without incurring Vault2Cloud™ fees.

26. How much data can I vault with Vault2Cloud™?

There is no single answer for this; it completely relies upon your WAN uplink speed, the amount of WAN bandwidth you are willing to commit to vaulting, your data change rate, the model of on-premise appliance you have, and other factors. In terms of general guidelines, we have created a table of recommendations based on a high quality WAN uplink connection, an average data change rate, and an average compression rate, and our current generation of on-premise data protection appliances.

Uplink and Uplink Speed	Daily Uplink % Dedicated to Vaulting	Recommended Protected Data Amount	Estimated Time to Seed without RapidSeed™
200 Kbps	33% - 100%	Up to 100GB	3-10 Weeks
512 Kbps	33% - 100%	Up to 250GB	3-10 Weeks
768 Kbps	33% - 100%	Up to 400GB	3-10 Weeks
1 Mbps	33% - 100%	Up to 500GB	3-10 Weeks
1.54 Mbps	33% - 100%	Up to 800GB	3-10 Weeks
3 Mbps	33% - 100%	Up to 1.5TB	3-10 Weeks
5 Mbps	33% - 100%	Up to 2.5TB	3-10 Weeks
10 Mbps	33% - 100%	Up to 5TB	3-10 Weeks

Note that the estimated time to seed without RapidSeed™ assumes 33% of the uplink for the higher end of the range and 100% of the uplink for the lower end of the range.

27. How is Vault2Cloud™ priced?

Pricing is \$0.49 per month per protected gigabyte in 100GB increments.

28. How often am I billed for Vault2Cloud™?

You are billed once a quarter.

29. What happens if I don't pay my bill?

Your access to Vault2Cloud™ will be denied.

30. Do I lose my data if I don't pay my bill? How long do I have before I lose my data? Is there a reconnection fee?

Eventually you will lose your data. Specific terms and conditions are stated in your Vault2Cloud™ contract.

31. Does Vault2Cloud™ offer a way to rapidly seed data so that I can protect my on-premise data in hours rather than in weeks or months?

Yes. This is an optionally available service called RapidSeed™.

For more detailed questions regarding the seeding process, see the appropriate questions in the remainder of this document.

32. How much does RapidSeed™ cost?

RapidSeed™ is priced at \$995.

33. If I significantly change the data being protected, will I need to perform RapidSeed™ again?

It depends upon the amount and your tolerance for the length of time that your system is being seeded; however, if you need more data uploaded in a shorter amount of time than your uplink WAN bandwidth is allows then you will need to rapid seed again.

34. How do I install Vault2Cloud™ capability for my on-premise data protection appliances?

Unitrends performs the initial installation remotely.

35. Is there any required installation fee?

No.

36. Is Vault2Cloud™ data transmission secure?

Yes. Vault2Cloud™ requires the use of OpenVPN. OpenVPN uses OpenSSL to perform all encryption and authentication work.

37. Does Vault2Cloud™ require OpenVPN to run over UDP?

Yes. Vault2Cloud™ requires that OpenVPN run on UDP. TCP-based OpenVPN is not supported by Vault2Cloud™.

38. Does Vault2Cloud™ offer storage-based encryption?

Vault2Cloud™ provides storage-based encryption through the encryption capabilities of the on-premise data protection appliance. Encryption must be enabled on the on-premise data protection appliance.

39. Is the data facility in which my vaulted data is housed SAS70 compliant?

Yes.

40. How is my disaster recovery data protected “in the cloud” in case there is a disaster at my site and at the same time a problem with the equipment “in the cloud” am I covered?

Yes. The vaults that are in the cloud have secondary single site protection as well.

41. Is there sufficient incoming and outgoing bandwidth to the data facility that hosts the cloud?

Yes. There are multiple, redundant, OC-192 connections.

42. In the case of disaster, how do I recover my data?

If you have RapidReplacement™ for all of your appliances, you notify Unitrends of the disaster and we arrange next-day shipping of replacement data protection appliances for all of your on-premise data protection appliances. These replacement appliances will have the data that you last protected via Vault2Cloud™. You can use those replacement appliances to restore all of your on-premise protected appliances.

If you don't have RapidReplacement™, then you will need to order replacement on premise appliances from Unitrends. Once you receive those appliances, you can restore them using the data that you last protected using Vault2Cloud™ - however, it should be noted that depending on the amount of data this restore may take weeks or months to occur.

43. How is RapidReplacement™ priced?

RapidReplacement™ is priced as a level of service available from Unitrends. The price is 21% of protected on-premise appliance prices for a one-year contract.

44. Is cross-vaulting available with Vault2Cloud™?

No. Customers who desire to cross-vault should use private vaulting.

45. Does Vault2Cloud™ offer retention?

No. Vault2Cloud™ is a disaster-recovery service only.

PROTECTING DATA

46. What types of data can I protect with VaultToCloud™ or private vaulting?

You can protect every form of data that Unitrends protects with its on-premise appliance with the sole exception of selective backups. This means that you can protect BareMetal, master, incremental, Exchange, SQL, and general storage. In addition, the metadata associated with the on-premise appliance is also protected – this is known as “System State.”

47. Can I protect BareMetal backups with VaultToCloud™ or private vaulting?

Yes. You can also exclude BareMetal backups from vaulting in order to optimize both your vaulting license and the amount of used bandwidth on the WAN.

48. Can I protect master and incremental backups with VaultToCloud™ or private vaulting?

Yes.

49. Can I exclude master and incremental backups from VaultToCloud™ or private vaulting?

You can exclude master and incremental backups from vaulting only by excluding the client itself from vaulting.

50. Can I protect selective backups with VaultToCloud™ or private vaulting?

No. Selective backups are not eligible for vaulting.

51. Can I protect Exchange backups with VaultToCloud™ or private vaulting?

Yes. You can also exclude Exchange backups from vaulting in order to optimize both your vaulting license and the amount of used bandwidth on the WAN.

52. Can I protect SQL backups with VaultToCloud™ or private vaulting?

Yes. You can also exclude SQL backups from vaulting in order to optimize both your vaulting license and the amount of used bandwidth on the WAN.

53. Can I protect general storage with VaultToCloud™ or private vaulting?

Yes. In some of our literature, this is known as “Local Directory” protection.

54. Do I need an on-premise appliance in order to vault with VaultToCloud™ or private vaulting?

Yes. Unitrends requires an on-premise appliance for local data protection, retention, and the intensive work of data reduction (via in-flight data deduplication), and other functions.

55. Can I configure my servers or PCs with the Unitrends agent to send data directly to the off-premise appliance (in the case of private vaulting) or to VaultToCloud™?

No. The process of reducing the amount of data that is required to lower WAN utilization is highly resource intensive and requires the on-premise appliance.

56. What is RapidSeed™?

RapidSeed™ is the capability of transferring a large amount of data from the on-premise appliance to the off-premise appliance. RapidSeed™ may be used the first time a vaulting-enabled on-premise appliance is put in service. RapidSeed™ may also be used when one or more customer computers with a large amount of storage that are being protected by an on-premise appliance undergo an atypical change in that storage (e.g., a decision is made to add or delete a large amount of storage on that computer.) RapidSeed™ may also be used when a network failure occurs of such duration that the vaulting process over the WAN may not reasonably recover within an appropriate timeframe and no more WAN bandwidth is available to overcome that issue.

If you have private vaulting, then you will perform RapidSeed™ yourself. If you have Vault2Cloud™, then you must contact Unitrends to perform the RapidSeed™ service.

Background: Storage amounts are growing rapidly; WAN speeds are not. Vaulting would be much simpler if the WAN between the on-premise appliances and the site at which the off-premise appliance was located was as fast as the LAN within the local premises. Unfortunately, while on-premise LANs are typically at least 100Mbps or 1Gbps, common WAN circuits such as T1 only offer 1.5Mbps. Seeding is born out of the

discrepancy between rapidly growing storage amounts, high-speed LANs, and much slower and more expensive WANs.

57. What is the alternative to RapidSeed™?

Yes. You can simply seed using your WAN. This can take a significant amount of time (for example, 500GB to 1TB of data can take weeks to months to seed.)

58. What is in-flight data deduplication?

In-flight data deduplication is the process by which the on-premise appliance and vault (whether that vault is privately owned or hosted in the Vault2Cloud™ service) work together to decrease the amount of data that has to be sent over the WAN. This is done by examining all of the data that is to be sent to the vault against data that was previously sent to the vault and eliminating duplicate blocks of data so that they don't consume precious WAN bandwidth.

You can view the data reduction achieved by in-flight data deduplication using the report system of the RRC.

59. What happens with respect to vaulting if the encryption passphrase is changed?

The purpose of encryption is to change all of the underlying data in order to offer protection against data theft. When the encryption passphrase is changed it means that all of the underlying data must change as well. This means that all of the data must be sent to the vault again - which will take an enormous amount of time. Thus any time an encryption passphrase is changed for a vaulted client a great deal of planning and care must be taken since in essence that data will need to be seeded again.

60. Is there a difference between data being modified, created, and deleted through normal user interaction and data being modified, created, and deleted through large movements of data from one customer computer to another?

No.

61. What happens with respect to vaulting if a large amount of data is deleted on a client being protected by vaulting?

This means that the incremental change rate will be high and quite possibly a great deal of data deduplication time will be spent processing the changes both on the on-premise appliance and on the vault.

62. What happens if a large amount of data is copied onto a client being protected by vaulting?

This will result in a large change in the amount of data needing to be processed and quite possibly a large amount of data needing to be sent via the WAN.

63. Can I split my master (through the use of exclusion lists) so that one master is vaulted while another is not?

No you may not – or at least, you may not on a reliable basis. If vaulting is enabled for a client then the last master available will always be vaulted.

64. Does private vaulting or Vault2Cloud™ support retention?

The vault only supports the last master and last incremental. The vault is not an archival device; it is a disaster recovery device.

65. What features are provided for longer-term data archiving?

Longer-term data archiving is achieved from the on-premise appliance through disk-based archiving (D2D2D.) Disk-based archiving is available on all of our on-premise appliances; the specific device that is used depends upon the model of on-premise appliance. Devices supported include

- eSATA (External SATA.) Some of our on-premise appliances have support for an external SATA-based device via a connector known as eSATA.
- SATA (Internal SATA.) Some of our on-premise appliances have support for what is termed the SDA (Single Drive Archive) which is a single hot plug drive in the appliance that is used for archiving.
- Infiniband. Some of our older on-premise appliances have support for our MDA (Multi-Drive Archive) device which is connected to the on-premise appliance via Infiniband. This has been replaced by our Recovery-Archive appliance which uses eSATA.
- Third-party tape. Some of our on-premise appliances have a parallel SCSI connector for use with third-party tape devices.

66. Can a single backup appliance vault to two private vaults? Can a single backup appliance vault to a private vault and Vault2Cloud?

No. A single backup appliance can vault to one and only one private vault or conversely only to Vault2Cloud.

MANAGEMENT AND MONITORING

67. Can I monitor what has been vaulted?

Yes. Both the status and reporting systems of the RRC may be used to monitor what has been vaulted.

68. Can I monitor multiple on-premise appliances from a vault in private vaulting?

Yes. Logging onto the RRC of the vault enables the user to monitor all of the on-premise appliances that are registered for vaulting to a vault. Note that if you are using Vault2Cloud™ you do not have the ability to directly manage or monitor the vault; instead, you manage and monitor vaulting from your on-premise appliance.

69. Can I manage multiple on-premise appliances from a vault in private vaulting?

Yes. Logging onto the RRC of the vault in private vaulting enables the user to manage all of the on-premise appliances that are registered to vault to an off-premise appliance. Note that if you are using Vault2Cloud™ you do not have the ability to directly manage or monitor the vault; instead, you manage and monitor vaulting from your on-premise appliance.

70. Can I manage multiple off-premise appliances, on-premise appliances, and clients from a single vault in private vaulting?

You can manage multiple on-premise appliances and clients from a single vault in private vaulting; you can't manage other vaults from a single vault in private vaulting.

71. If I am using private vaulting, are there management features that are different for the on-premise appliance if I log in directly to the on-premise appliance versus if I log in to the vault to manage one or more on-premise appliances?

Yes; there are several features that for security reasons are only available locally on the on-premise appliance. Examples are changing the system root password (not the RRC passwords, but the underlying system root password of the appliance), changing port, performing a software shutdown of the on-premise appliance, granting permission to be managed by an off-premise appliance, and burning encryption keys onto the local on-premise appliance's optical storage.

72. Can I control how much bandwidth is used for vaulting in private vaulting or in Vault2Cloud™?

Yes. The RRC contains a throttling control that allows maximum bandwidth to be set on an hourly basis for each day of the week.

73. Can I block out specific times in which vaulting will not use the WAN in private vaulting or in Vault2Cloud™?

Yes. The RRC contains a throttling control that allows a maximum bandwidth of zero (or higher values, for that matter) to be set on an hourly basis for each day of the week.

74. What status and report tools are available with respect to vaulting in private vaulting or in Vault2Cloud™?

There is a detailed monitoring and management section of the RRC from which vaulting can be monitored and managed.

The first screen of the user interface (the RRC) offers a snapshot of vaulting in its RRC status system and offers a detailed vaulting report in its RRC report system.

There is also an in-flight data deduplication report that shows the data reduction achieved in vaulting.

75. What tools does Unitrends provide on the on- and off-premise appliances to help me monitor my network and diagnose issues if I am using private vaulting?

Unitrends includes the following open source tools to help resellers and customers diagnose underlying network issues:

- Network monitoring: ntop
- Network performance: iPerf
- Network troubleshooting: Wireshark
- VPN (network fault tolerance and single port multiplexing): OpenVPN

Please note that if you have a release made before release 4.1, all of these are widely available on the Internet and all are free open source tools.

76. Are SNMP traps supported on my on-premise appliance (in private vaulting and in Vault2Cloud™) and on my vault (in private vaulting)?

Yes.

77. Do the on-premise appliances (in private vaulting and in Vault2Cloud™) support any third-party MSP (Managed Service Provider) platforms?

MSP platform support is available at this time through either SNMP traps or via “scraping” techniques of various logs.

78. Do the on-premise appliances (in private vaulting and in Vault2Cloud™) support any third-party PSA (Professional Service Automation) platforms?

PSA platform support is available at this time through either SNMP traps or via “scraping” techniques of various logs.

RECOVERING FROM AN EVENT

79. What is the difference between event recovery and disaster recovery?

Disaster recovery refers to a natural or human-based disaster in which all (or virtually all) of the infrastructure of a customer’s premises are lost. When a disaster occurs, the customer must replace their physical infrastructure. When an event occurs, the customer for some reason may lose “only” some section of their physical infrastructure. Typically an event is recovered completely through the use of the on-premise appliance. However, there are some events in which it is necessary to recover some data from the vault.

80. Can I recover a file remotely in private vaulting or in Vault2Cloud™?

Yes; use the RRC (Tools -> Restore from Vault). This brings the file back to the on-premise appliance as a selective backup from which you can perform the standard recovery operation to restore the file to a customer’s computer.

81. Can I recover a directory remotely in private vaulting or in Vault2Cloud™?

Yes; use the RRC (Tools -> Restore from Vault). This brings the directory back to the on-premise appliance as a selective backup from which you can perform the standard recovery operation to restore the directory to a customer’s computer.

82. Can I recover a volume remotely in private vaulting or in Vault2Cloud™?

Yes; use the RRC (Tools -> Restore from Vault). This brings the volume back to the on-premise appliance as a selective backup from which you can perform the standard recovery operation to restore the volume to a customer’s computer.

83. Can I recover a single customer computer remotely in private vaulting or in Vault2Cloud™?

No. The remote recovery tools are file, directory, and volume based; recovery of an entire computer should be done locally.

84. Can I recover a single customer computer locally using private vaulting?

Yes.

85. What do I do about auditing an event recovery in private vaulting or in Vault2Cloud™?

The goal of auditing an event recovery is to prove that you can restore a file, directory, or volume. We have customers, particularly but not limited to financial institutions, who have asked for the ability to audit event recovery through proving that they can restore a file, directory, or volume from the vault to the on-premise appliance to the client computer.

Auditing event recovery is fairly simple: use the RRC (Tools -> Restore from Vault) to restore a file, directory, or volume to the on-premise appliance and use the standard restore processes to restore that file, directory, or volume from the on-premise appliance to a customer's computer. This satisfies auditing requirements that you prove you can recover from an event by recovering a file, directory, or volume.

RECOVERING FROM A DISASTER (REPLACING THE ON-PREMISE APPLIANCE)

86. How do I recover in the case of a disaster whether I use private vaulting or Vault2Cloud™?

What governs the methodology by which you recover is your DRP (Disaster Recovery Plan.) There are an incredible number of schemes that may be used in a DRP, but the most important factor is how quickly you require that your business be functioning after the disaster.

87. What is the best practice for using our on-premise appliances and vaults (private vaulting) or Vault2Cloud™ for the fastest possible recovery in the event of a disaster?

With respect to private vaulting, if the desire is to recover in a day or less, then the vaulting site should have spare chassis for every on-premise appliance that must be recovered and have those set up in an existing infrastructure at the vaulting site. When a disaster occurs, the on-premise appliances are then restored from the off-premise appliance, and the computers in the existing infrastructure are restored from the on-premise appliances.

With respect to Vault2Cloud™, you should use RapidReplacement™. This service is described in more detail in the Vault2Cloud™ section of this document.

88. How quickly can I get a replacement on-premise appliance in the event of a disaster?

You can get a replacement on-premise appliance as quickly as overnight. However, in terms of analyzing the amount of time it will take to recover from a disaster, you must also count the time not only to receive an on-premise appliance but the time to restore that on-premise appliance from the vault. Since the vault may be in a separate location (note: the location of the disaster recovery premises is a decision made during disaster

recovery planning that has occurred previously) the time it takes to not just receive the replacement on-premise appliance but to restore it must be planned.

89. Can I recover from a vault to an on-premise appliance that has a different release of software?

Yes. The vault may have a later release of software than the on-premise appliance and recovery of data from the vault will not be affected.

90. Do I have to have the same version of software on my replacement on-premise appliance as my original on-premise appliance?

Yes. Part of what is vaulted from the on-premise appliance to the off-premise appliance is the “personality” of the on-premise appliance (also called “metadata” or “system state.”) This changes from release to release and thus the replacement on-premise appliance must have the same version of Unitrends software as the on-premise appliance that is being replaced.

SCALING AND PROVISIONING

91. How many clients will one on-premise appliance support?

Unitrends publishes either maximum numbers of clients an on-premise appliance can support on a licensed basis or it publishes a recommended number of clients. These differ based upon the type of on-premise appliance.

Strictly speaking, however, there is no single answer for this; an on-premise appliance can support thousands of clients or an on-premise appliance can support only a few (or one) clients. It is more helpful to ask how much data one on-premise appliance can support. The amount of data an on-premise appliance can support is limited by a number of factors that include the performance of each client, the available LAN bandwidth, and the activity level of the on-premise appliance itself (e.g., whether the on-premise appliance is encrypting data, is vaulting, is cross-vaulting, etc.)

92. How many on-premise appliances will one vault support in private vaulting?

There is no single answer for this; an off-premise appliance can support as many as 63 on-premise appliances or a vault can support only a few (or one) on-premise appliance. It is more helpful to ask how much data one vault can support. The amount of data a vault can support is limited by a number of factors that include the incremental data change rate of each on-premise appliance and the available WAN bandwidth.

93. How many on-premise appliances will Vault2Cloud™ support?

Vault2Cloud™ is an inherently scalable platform; it will support as many on-premise appliances as you have.

94. How many clients will one vault support?

With respect to private vaulting, there is no single answer for this; a vault can support thousands of clients or a vault can support only a few (or one) client. It is more helpful to ask how much data one vault can support. The amount of data a vault can support is limited by a number of factors that include the incremental data change rate of each on-premise appliance and the available WAN bandwidth.

With respect to Vault2Cloud™, the answer is driven entirely by factors that include the incremental data change rate of each on-premise appliance and the available uplink WAN bandwidth.

95. I have vault (in private vaulting) and/or on-premise appliance hardware (in either private vaulting or Vault2Cloud™) that are a few years old; will that negatively impact my vaulting performance?

Yes. In-flight deduplication is resource intensive in terms of a processor, memory, storage, and I/O performance. If your hardware is a few years old, then the chances are that the currently shipping processor (for example) is an order of magnitude higher performance than your hardware.

96. What's more important for vaulting performance – my on-premise appliance performance, my WAN bandwidth, or my vault performance?

Of these three factors typically the most important factor for vaulting performance is WAN bandwidth. However, as WAN bandwidth increases, the second-most important factor then becomes on-premise appliance performance. Typically vault performance is only a tertiary factor with respect to vaulting performance.

97. Is there no way to roughly estimate how much data a vault can protect given the unique characteristics of my environment for private vaulting?

Your Unitrends sales person and sales support person has access to a vaulting estimation calculator that they can use to very roughly approximate a range of scenarios in terms of vaulting data protection.

98. What about the underlying operating system type? Should my appliance be operating on a version of RecoveryOS based on CentOS 5, CentOS 4, or Fedora Core 2?

The best choice is for your appliance's operating system (RecoveryOS) to be based on CentOS 5. There are upgrades available for your operating system; however, we **strongly** recommend that you closely examine an appliance upgrade rather than just an operating system or storage upgrade. If your hardware is a few years old, then the chances are that the currently shipping processor (for example) is an order of magnitude higher performance than your hardware – and this will greatly impact the amount of data you are able to protect.

99. Must the software release version match among my vaults (in private vaulting) and all vaulting on-premise appliances? What about in Vault2Cloud™?

[With respect to private vaulting]

No. The rules regarding software release versions are that one of the following must be true for all releases since release 4.0:

- The vault version must always be equal to the version of software on the on-premise appliance.

- The vault version must always be one version ahead of the version of software on the on-premise appliance.

Here's an example of this rule. If an off-premise appliance has release 4.0.3 installed, then an on-premise appliance with 4.1 will not operate on that off-premise appliance – the off-premise appliance must be upgraded to 4.1. If an off-premise appliance has release 4.1 installed, then it supports on-premise appliances with release 4.1 and 4.0.3 (the last version before 4.1) installed.

[With respect to Vault2Cloud™]

The rules are the same as above; however, as part of your Vault2Cloud™ agreement you will need to insure that the on-premise appliances you have are kept on the latest release of software.

100. What if I have a version of software that predates release 4.0? What do I do?

With respect to private vaulting, we **strongly** recommend that you upgrade to supported software. All versions of software prior to 4.0 are now officially desupported. For more information, please see customer portal at the Unitrends web site.

With respect to Vault2Cloud™, we do not support any appliances that are not running recent versions of software.

101. With respect to private vaulting, what is the best practice for installing software versions among a vault and all vaulting on-premise appliances?

The best practice is to install new versions of software as quickly as possible on the vault and then bring all on-premise appliances up to that version as soon as possible. Each release of software typically seeks to increase the performance and the fault tolerance of vaulting and for best results.

102. What are the primary factors that affect how much customer data can be vaulted in either private vaulting or Vault2Cloud™?

Typically the most important factor for vaulting performance is the combination of the amount of customer data to be vaulted, the change rate associated with that data, and the WAN bandwidth. However, as WAN bandwidth increases, the second-most important factor then becomes on-premise appliance performance. Typically off-premise appliance performance is only a tertiary factor with respect to vaulting performance.

103. What are the transport types available in private vaulting and Vault2Cloud™?

For private vaulting, the transport types available for vaulting are “sockets” and “ssh.” For Vault2Cloud™, the only transport type available is “sockets.” See the next question for more detail.

104. Is there a preferred transport type for private vaulting and Vault2Cloud™?

For private vaulting, the preferred transport type is “sockets” implemented over a UDP-level VPN. We strongly recommend OpenVPN, a free and open source VPN program.

For Vault2Cloud™, we require the use of OpenVPN implemented over a UDP-level VPN.

105. How do I secure the network between my vault and my on-premise appliances (in private vaulting) or between Vault2Cloud™ and my on-premise appliances?

For private vaulting, the best mechanism for doing this is to establish a VPN (Virtual Private Network) running on the UDP protocol layer. We recommend OpenVPN, a free and open source VPN program.

For Vault2Cloud™, we require the use of OpenVPN implemented over a UDP-level VPN.

106. What is the performance impact of using “sockets” over a VPN versus using “ssh?”

All things being equal, the performance of “sockets” over a VPN is typically slightly faster than an “ssh” implementation. Of course, this depends upon the actual implementation of the VPN.

However, all things are typically not equal. The most important factor associated with vaulting performance in terms of transport type is the reliability of the underlying networking. If a session is terminated (sometimes called “dropped”), vaulting must restart completely. A UDP-level VPN solution (such as OpenVPN) allows vaulting to have a much better chance of successfully handling minor disruptions in the underlying networking protocol.

107. What is the security impact of using “sockets” over a VPN versus using “ssh?”

It depends upon the actual security implementation of the VPN. OpenVPN tends to be much more secure.

108. What is the quality impact of using “sockets” over a VPN versus using “ssh?”

If a UDP-level VPN is used, the “sockets” transport type is selected, and all vaulting traffic is assigned to using the VPN, then the quality of “sockets” is much higher than “ssh” because of the ability of UDP-level VPN to better handle short-lived transient line failures.

109. What type of WAN do I need to vault in private vaulting and with Vault2Cloud™?

On the on-premise appliance side, the WAN must have enough upload capacity for the amount of data to be protected and it must have sufficient quality. This applies with either private vaulting or Vault2Cloud™.

With respect to private vaulting, on the vault side, the WAN must have enough download capacity for the amount of data to be protected from all on-premise appliances that vault supports.

With respect to Vault2Cloud™, on the vault side, this is the responsibility of Unitrends. Please see the Vault2Cloud™ section for more details regarding the implementation of our cloud.

110. What is the best WAN for vaulting from the on-premise appliance side.

The best WAN for vaulting is a WAN with the most bandwidth and the highest quality. For most of our customers, the best WAN for vaulting is a T3 or higher. However, due to WAN circuit cost considerations, we have quite a few customers using bonded T1s (multiple T1s that act together to provide higher bandwidth.)

111. What is the worst WAN for vaulting from the on-premise appliance side.

There really is no “worst” WAN for vaulting. The only major issue is whether you want to protect more data at a higher data change rate than your WAN uplink speed can support.

Thus the worst WAN for vaulting is a WAN with the lowest bandwidth and the lowest quality. Quite often this is consumer-grade cable or DSL unless special provisions are made to insure appropriate guaranteed upload and download bandwidth and high quality.

112. What is an “asymmetric” WAN? Can I use one for vaulting?

An asymmetric WAN is one which has a different download and upload speed. You can use an asymmetric WAN for vaulting as long as you understand the difference between the download and upload speed and how it may impact vaulting. If the WAN being used at the site of the on-premise appliance has a download speed of 10Mb/s and an upload speed of 1Mb/s, then protection for that site will be limited by a maximum of 1Mb/s since most data has to move from the on-premise appliance’s site to the vault’s site or to Vault2Cloud™. However, file, directory, or volume recovery will operate at a maximum of the 10Mb/s rate since recovery moves data from the vault site or Vault2Cloud™ to the on-premise appliance.

If you are using private vaulting and if the asymmetric WAN is provided at the site of the vault, then the directionality is reversed.

113. What is the most common WAN used in vaulting?

The most common WAN used in vaulting are bonded T1s and T3s. Customers on a budget may use T1s. Unitrends recommends in most cases that customers minimally use T1s for private vaulting. For Vault2Cloud™, the customer may use any WAN that has uplink speed and quality necessary to support the desired data amount and data change rate.

114. Can I use a fractional T1 for private vaulting or for Vault2Cloud™?

Yes; however, the amount of data that can be protected will be limited.

115. Can I use cable or DSL for vaulting?

Yes; however, the amount of data that can be protected will be limited.

Great care needs to be taken with respect to the amount of bandwidth that will actually be available to protect your data. Time Warner Cable, for example, advertises a premium service at 8Mb/s. However, this is an “asymmetric” bandwidth rating – which means that the download performance is different than the upload performance. The upload performance for Time Warner Cable for this premium 8Mb/s service is actually 512Kb/s – equivalent to a fractional T1 (1/3 of a T1.) In addition, this is peak upload bandwidth – performance

on cable suffers with more users. DSL is less prone to degradation due to additional users, but typically its overall performance is slower as well.

116. How much bandwidth do I need to vault in private vaulting?

This is an incredibly complex question to answer. There are a number of primary factors involved in calculating this ranging from the amount of data to be vaulted, the change rate of that data, the amount of replicated blocks in that data that are subject to de-duplication, the quality of the network, and the length of time available for vaulting to occur. As the amount of bandwidth increases, there are secondary factors associated with on-premise appliance performance and tertiary factors associated with off-premise appliance performance.

Unitrends can help you in answering this question through an audit of your current environment; please see your Unitrends representative for more information.

117. How much bandwidth do I need to vault in Vault2Cloud™?

Please see the answer to this question in the Vault2Cloud™ section.

118. Does my network need to be dedicated to vaulting for either private vaulting or Vault2Cloud™?

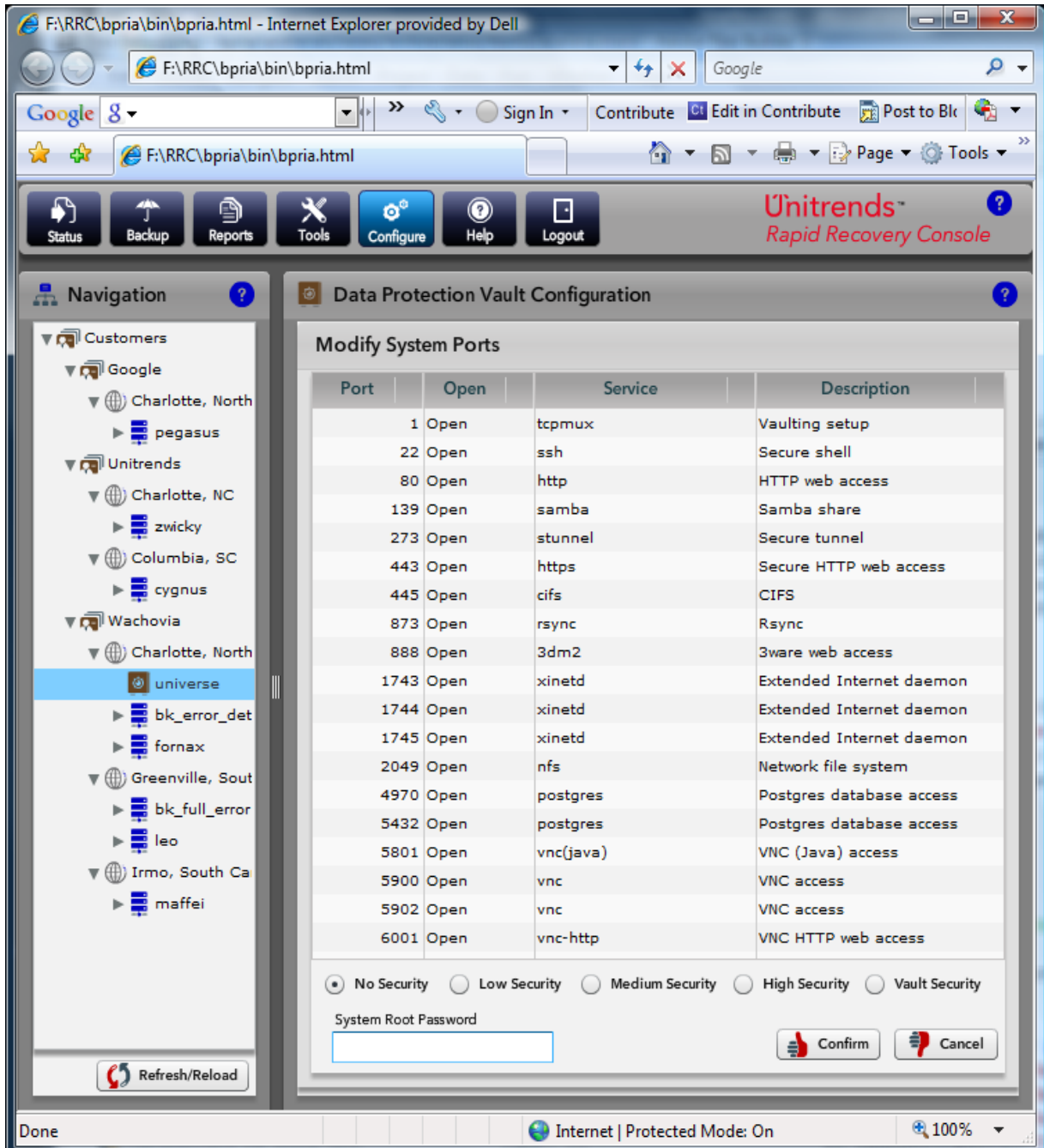
No; however, sufficient bandwidth must be available for the transfer of data from the on-premise appliance to the vault. It is possible at the on-premise appliance to “throttle” the maximum amount of bandwidth available for vaulting. It is also possible to use third-party networking products in order to statically or dynamically limit the amount of bandwidth available for vaulting (and/or to specify a minimum amount of bandwidth that must be made available for vaulting.) If such a third-party product is used, care must be taken that it not decrease the quality of the WAN. In other words, if the third-party networking product introduces session drops, it will dramatically reduce the efficacy of vaulting.

119. How many and which ports do I open to use Vault2Cloud™?

You only need one port open to use Vault2Cloud™. The person who contacts you to install this on your system will work with you to open that single port in the proper configuration.

120. What are the ports used among the vault and on-premise appliances in private vaulting?

The following is a screenshot from the RRC: Configuration -> Ports; it shows all of the ports used on the on-premise appliances and vaults. Please note that this does not include a specific port to be opened for OpenVPN; if that was the case then of course these ports would be multiplexed onto the OpenVPN port.



121. I don't want to open ports in my firewall; why can't I use just one port?

[With respect to private vaulting]

Not only can you – we strongly recommend that you do so. To use one port, use a VPN with the transport layers set as “sockets.” This is the recommended approach. If a VPN has not yet been selected, we recommend OpenVPN configured to run at the UDP level.

[With respect to Vault2Cloud™]

You will only be able to use one port since you must use OpenVPN.

122. How well does vaulting work with a heavily congested network?

Vaulting was designed to work on shared networks and offers features such as “throttling” that allow vaulting to be constrained to only specified limits of bandwidth that may be set on an hourly basis on a weekly period. Of course, the amount of bandwidth available (and the amount of data that is to be protected coupled with the change in that data on a daily basis) will drive a requirement for bandwidth – so the actual capacity of vaulting on a heavily congested network will be determined by the amount of aggregate bandwidth available on that network.

123. Can I use ToS/QoS (Terms of Service/Quality of Service) with vaulting?

Yes. You may use your existing networking equipment and use various networking commands to adjust on a per-port basis the latency and other characteristics of different vaulting services. However, please note that this is a very advanced topic and should be attempted only if you possess a great deal of networking expertise.

124. Can I use a WAFS (Wide Area File Services) or WO (WAN Optimization) product with private vaulting?

Yes; however, please see the next question for details concerning this.

125. How well do WAFS/WO products work with private vaulting?

WAFS/WO products work by essentially caching and de-duplicating data. Because vaulting already de-duplicates data, and because vaulting typically involves the movement of more data than WAFS/WO products have cache to hold, WAFS/WO products don't typically show a great deal of improvement in increasing vaulting effectiveness. In addition, some WAFS/WO products require a relatively static port usage profile for operation while vaulting uses a relatively dynamic port usage profile.

However, vaulting works well with WAFS/WO products in terms of co-existing with these products and allowing other forms of WAN bandwidth to be optimized.

126. Will I get any benefit from using a WAFS/WO product with Vault2Cloud™?

Since that WAFS/WO product won't have a paired product at the Vault2Cloud™ site, it will not increase effective WAN bandwidth rate.

127. What can cause the vaulting process to be interrupted?

The most common cause of vaulting process interruptions are WAN session failures. This means that a vaulting session is abnormally terminated because the TCP protocol layer upon which vaulting depends is itself terminated due to an underlying protocol failure. This failure may be caused by something as serious as a construction crew accidentally cutting through the WAN circuit to something as trivial as someone stepping on an unsecured cable in the back office where the vault or on-premise appliance resides. Less common causes are a hardware or software failure in the vault or on-premise appliance itself.

128. How can I prevent the vaulting process from being interrupted?

The best way to prevent the vaulting process from being interrupted is to ensure that you have an SLA from your WAN (sometimes called “circuit” provider) that calls for a very high-quality connection, that you use redundant techniques that allow for a route to always exist between the vault and the on-premise appliance, and to use a UDP-level VPN (such as OpenVPN) to create additional fault tolerance for very short-lived transient network failures.

129. What happens if the vaulting process is interrupted?

It completely depends upon the phase of the vaulting process in which the interruption took place. There are times in which a vaulting process interruption has little or no effect on the vaulting process. In versions of our software released before release 4.1.2, the worst case is that a large transfer that has almost completely finished will have to completely restart. In all versions since that time, the worst case is that the last 1MB of transferred data will have to be retransferred.

LICENSING

130. What tools does Unitrends provide to enable monitoring and management of the licensed storage in private vaulting?

Unitrends provides a report via the RRC that depicts the actual versus licensed storage for the vault on an aggregate basis and depicts usage on a per- on-premise appliance basis.

131. What tools does Unitrends provide to enable monitoring and management of subscribed storage in Vault2Cloud™?

Unitrends provides a report via the RRC that depicts the backups and the associated size of those backups that have been vaulted.

132. Does Unitrends enforce vault licensing in private vaulting?

Not at this time; however, Unitrends will begin enforcing vault licensing in release 5.

133. What is the difference between a BareMetal-based backup and a master-based backup?

A BareMetal is an image-based backup and a master is a structured and unstructured data based backup (e.g., files.)

134. How does licensing (private vaulting) or my Vault2Cloud™ subscription take into account a BareMetal-based backup and a master-based backup that protects the same volume?

The BareMetal-based backup is counted separately from the master-based backup; you must add both against your protected system content.

135. What is the best practice for optimizing license space with respect to BareMetal and master backups?

The system volume should be dedicated to system activity and other volumes created for all other activity. (Note: This is typically recommended practice in any case because it improves system performance.)

136. Can I exclude clients to optimize my licensed vault space (private vaulting) or my subscribed vault space (Vault2Cloud™)?

Yes. Clients as well as different types of backups may be excluded in order to optimize your off-premise appliance license space.

137. Can I exclude BareMetal backups to optimize my licensed vault space (private vaulting) or my subscribed vault space (Vault2Cloud™)?

Yes.

138. Can I exclude Exchange backups to optimize my licensed vault space (private vaulting) or my subscribed vault space (Vault2Cloud™)?

Yes.

139. Can I exclude SQL backups to optimize my licensed vault space (private vaulting) or my subscribed vault space (Vault2Cloud™)?

Yes.

140. Can I exclude general storage (“Local Directory”) to optimize my licensed vault space (private vaulting) or my subscribed vault space (Vault2Cloud™)?

Yes.

VSP: VAULTING SERVICE PROVIDER USING PRIVATE VAULTING

141. What is a VSP?

A VSP (Vaulting Service Provider) is a type of MSP (Managed Service Provider) that offers vaulting using Unitrends appliances. A VSP has a private vaulting setup.

142. What is the relationship between Unitrends and a VSP?

Unitrends supplies appliances to VSPs and supports those appliances via its DA/DAP support contracts. We deliver and support the technology that helps our channel partners achieve their business objectives and meet customers’ vaulting and disaster recovery requirements.

143. Does a VSP have access to encrypted data that is vaulted?

No; not unless the customer of the VSP shares the customer's encryption passphrase with the VSP.

144. Can a VSP see the metadata (e.g., filenames, pathnames, backup operations, vaulting operations) associated with encrypted data?

Yes. This allows the VSP to monitor and manage data protection without having access to the encrypted contents.

145. Should a VSP stock spare chassis of each model of on-premise appliance that it sells?

It depends upon the SLA that the VSP has with the VSP's customer; but in most cases the answer is "yes."

146. Why should a VSP stock spare chassis of each model of on-premise appliance it sells?

To decrease the time it takes to create an appliance from the previously vaulted data and to ship that appliance to the VSP's customer in the case of a disaster.

147. Does Unitrends offer spare chassis for sale at very reasonable prices for this purpose to VSPs?

Yes.

148. Can Unitrends provide rack space or a co-location service to host my off-premise appliance?

No. Unitrends does not at this time offer rack space or co-location facilities.

149. Can Unitrends help me find a VSP with whom I can partner to sell vaulting services?

Yes. We have VSP partners located across the country that are running well managed vaulting services for an increasing number of very satisfied customers. Your Unitrends sales team can help you identify a VSP to meet your needs.

150. Do any of Unitrends VSPs offer SAS-70 compliant vaulting?

Not at this time.

151. Do any Unitrends VSPs offer cross-vaulting as a service?

No. Cross-vaulting is typically performed in private vaulting situations.

152. Does Unitrends recommend VSPs to use their vaults in either cross-vaulting or half-cross vaulting configurations?

No. VSPs typically have a stringent SLA associated with their services to their customers. It is recommended that VSPs dedicate their Unitrends appliance to the provision of the vaulting services associated with that SLA.

153. How does a VSP protect an off-premise appliance?

The off-premise appliance can only be protected using a separate on-premise appliance. If disaster recovery is desired for the off-premise appliance itself, then that on-premise appliance may be configured to vault to another geographic location or the on-premise appliance's archive capabilities may be used in an off-site rotation strategy.

154. Can a VSP manage and monitor on-premise appliances at a customer site while still allowing the customer to manage and monitor that on-premise appliance?

Yes. A VSP may manage and monitor on-premise appliances in one of two ways. The preferred way to do this is by logging into the RRC (Rapid Recovery Console) of the off-premise appliance and managing and monitoring the on-premise appliances registered to vault to that off-premise appliance in a "single pane of glass" interface. Another way to do this is by logging into the RRC of each individual on-premise appliance and managing and monitoring that on-premise appliance.

The customer may log into the on-premise appliance via the RRC and manage that individual on-premise appliance.

FUTURE DIRECTION QUESTIONS FOR PRIVATE VAULTING

155. Are you going to continue supporting private vaulting?

Yes.

156. E-mailed reports are not organized well and are not attractive; when will this be fixed?

A complete rewrite of our e-mail report system, bringing it in line with our RRC reporting standards, is scheduled for late 2010.

157. Do you have plans to support the backup of vaults in some method other than requiring a separate on-premise appliance in private vaulting?

We are currently evaluating this and will announce any such plans if such a decision is made.

158. Are there plans on supporting a SAN or NAS as attached storage to the vault in private vaulting?

There are no official plans; however, we are working with a few of our resellers with alpha versions of software that allow the attaching of SANs to vaults with Fiber Channel and iSCSI. The release date for general support of this functionality has not yet been set.

159. Are there plans on supporting SAN replication on attached storage to the vault in private vaulting?

There are no official plans; however, with our support of SANs we are exploring allowing replication between SANs. The release date for general support of this functionality has not yet been set.

MISCELLANEOUS

160. Must all on-premise appliances and vaults be the same appliance platform type in private vaulting?

No. Any on-premise appliance may vault to any off-premise vault appliance.

161. Is the data on the vault compressed?

No.

162. Why isn't the data on the vault compressed?

The data on the vault isn't compressed because it would slow down the "re-duplication" phase of the vaulting process.

163. Is the data on the off-premise appliance encrypted?

Yes, if the data were encrypted on the on-premise appliance before it was vaulted; no otherwise.

164. What type of encryption is offered on the on-premise appliance?

Unitrends uses a 256-bit AES form of encryption. Encryption is an optional feature.

165. Is there a maximum file size that can be protected on the on-premise appliance or vault (in private vaulting) or Vault2Cloud™? If so, what is it?

Yes. 4TB.

166. What is "rsync"?

Rsync is an implementation of an algorithm for efficiently transmitting data across a relatively low-speed transmission line when the receiving computer already has a different version of the same data.

167. What is "bpsync"?

"Bpsync" is an improvement of "rsync" which has better performance, better tolerance for network failures, and a higher degree of fault tolerance. "Bpsync" also has superior monitoring and management capabilities.

168. Does Unitrends use both "rsync" and "bpsync"?

It depends on the release of software; various versions of Unitrends releases concurrently use "rsync" and "bpsync" for different functionality.

- In release 4.0, Unitrends used "bpsync" for masters, incrementals, and baremetals.
- In release 4.0.1, Unitrends added "bpsync" for local directories and Exchange InfoStore.

- In release 4.1.1 and after, Unitrends added “bpsync” for on-premise appliance state and SQL backups. Thus in release 4.1.1, “bpsync” is used for all non-deprecated vaulting.

169.What is “DPU state?”

This is the personality (metadata) associated with the on-premise appliance. In order for Unitrends to restore an on-premise appliance, the personality of that on-premise appliance must be retained and restored.

170.What is “Secure Data Sync?”

Secure Data Sync is another name for vaulting. Secure Data Sync is an asymmetric replication feature that allows for data synchronization between one or more on-premise appliances to a single vault. Secure Data Sync permits the storage of mission-critical data to an off-site location; thereby protecting against loss of data in the event of a disaster.

171.Can one vault protect data from another vault in private vaulting?

Not directly. While an on-premise appliance can be used to protect an off-premise appliance, an off-premise appliance can't directly protect another off-premise appliance.

172.Are both vaults and on-premise appliances covered under my support contract in private vaulting?

Yes. All Unitrends appliances are covered under our maintenance and support programs if you have those services for the specific appliance. Services provided include software updates, support, and hardware warranty coverage.