WHITE PAPER

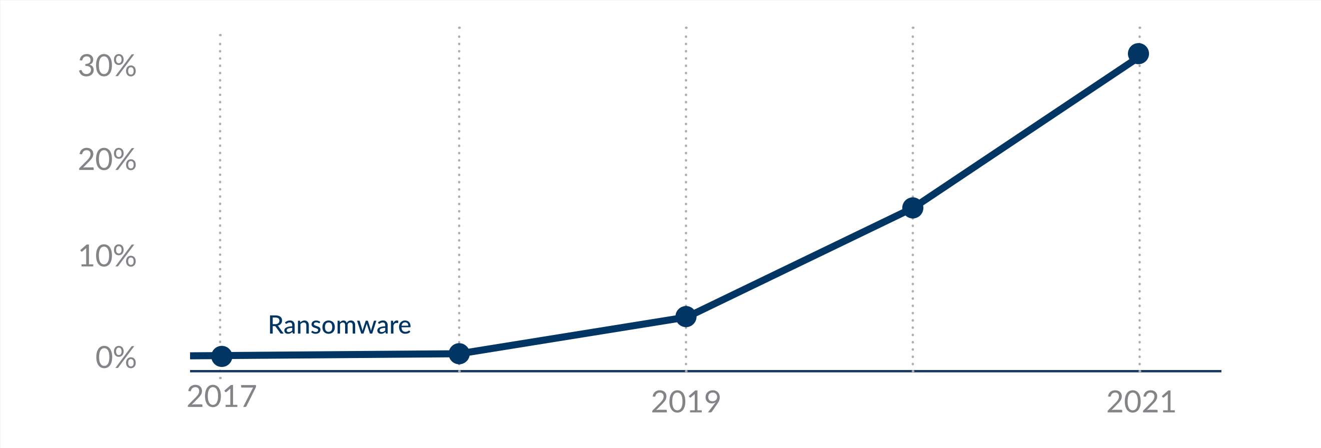
MSPs: 4-Minute Recovery with Nebulon TimeJump

How to Bring Your Customers Core Infrastructure Back to Life After a Ransomware Attack

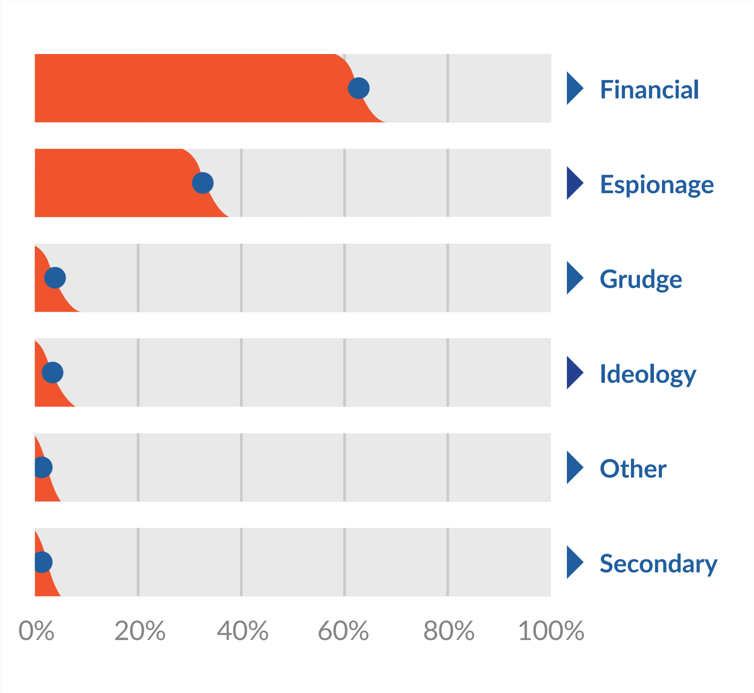
nebulon®

Ransomware is a type of malicious software planted in your customer's corporate network. Far from the indiscriminate destructive activity of many viruses, the goal of ransomware is financial gain for the perpetrators. This is typically accomplished by encrypting key data and extorting payment to restore access. Some groups will actively work to exfiltrate your customers data and sell it to the highest bidder on the black market or use it as leverage to extract an even greater payout. These attacks are successful because most businesses do not have a complete recovery plan and have not planned deeply enough for the "what if scenario", and sometimes have little choice but to pay the ransom and hope for the best.

Ransomware attacks are not isolated to any industry, but MSPs that have customers in education, defense, healthcare, and financial institutions should have deeper ransomware conversations with their customers. Any business that uses the Internet is a potential victim and the rate of attacks is increasing at a record pace. According to the Verizon 2022 Data Breach Investigations Report (DBIR) the number of ransomware attacks increased by 13 percent between 2020 and 2021 — a larger jump than the past five years combined.



Verizon 2022 Data Breach Investigations Report (DBIR)



Verizon 2022 Data Breach Investigations Report (DBIR)

Hackers and even nation-state actors have turned ransomware into a business, and business is good. According to the same report, approximately 65% of data breaches (where data was exfiltrated) were tied directly to financial gain.

According to the International Data Corporation (IDC), out of 500 organizations, 84% were victims of malicious attacks in 2019. Global ransomware damage costs were predicted to reach $20 billion (USD) by 2021, and to exceed $265 billion by 2031, according to Cyber Magazine[1]. With that kind of money in play, bad actors are increasing the sophistication of their attacks to cast a wider net.

[1] Cybercrime Magazine - Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031

MSP CONSIDERATIONS FOR DEFENSE-IN-DEPTH

To defend your managed services customers against external attacks, including ransomware, it is best to employ a defense-in-depth strategy to limit or contain the impact of a of a potential cybersecurity event. Firewalls, endpoint protection, multi-factor authentication, identity access, anti-malware software, employee education, and more are all critical components of a robust defense strategy.

However, to provide richer protection from ransomware, MSPs need to understand that hardening the outer shell of your customer's infrastructure is only part of the solution. According to the Verizon DBIR, 62% of attacks were classified as supply chain attacks. These attacks leverage weaknesses in software or services leveraged by both you and your customer's businesses to gain a foothold. The 2020 SolarWinds attack[2] which affected thousands of their customers is a prime example of this kind of strategy.

Moving your customer resources to the cloud does not guarantee safety either. According to Wanclouds[3], one in three AWS (Amazon Web Services) organizations lost data in the last year due to downtime incidents including those caused by cyberattacks. Every one of your customers has infrastructure exposed to the Internet and that makes it a target, no matter where it is hosted. For example, services like the Remote Desktop Protocol (RDP) are a sought-after entry point as they are susceptible to brute-force dictionary attacks. Given the increasing sophistication and proliferation of ransomware, an attack is a question of *when*, not *if*. This demands that every MSP offering managed infrastructure services, ask the question, "how will I recover my customer WHEN they get attacked?"

WHAT'S THE BLAST RADIUS?

It is impossible to know beforehand what parts of your customer's infrastructure might be compromised during a ransomware attack. Some attacks are automated and ham-fisted, spreading indiscriminately through their network, and some are more targeted data exfiltration campaigns. In either case, it is your responsibility to be able to respond to this situation without knowing exactly what state your customers core infrastructure will be in.

If the attack targets core infrastructure services such as DNS/DHCP or directory services, you may not be able to mount an effective response quickly. If DNS is down, that will cause cascading failures through the network. Failure of DHCP may leave many machines without valid IP addresses. Failures in directory services may mean you can't log in to important systems. Increasingly, ransomware incidents have started targeting backup systems and if you do not have offline backups, you may have no way to recover your customer data at all.

If you work with cyber insurance agencies in collaboration with your customer and are insured against ransomware attacks, you may have additional considerations before you can begin to recover your customers infrastructure. Your customer's insurance provider may require you to leave systems in their compromised state so they can confirm the attack and the extent of the damage, thereby delaying getting "back to business". If data is only encrypted and not deleted, you may be denied remuneration by your provider.

[2] TechTarget – SolarWinds Hack Explained: Everything You Need to Know

[3] Wanclouds - Disaster Recovery and Resilience Survey 2021

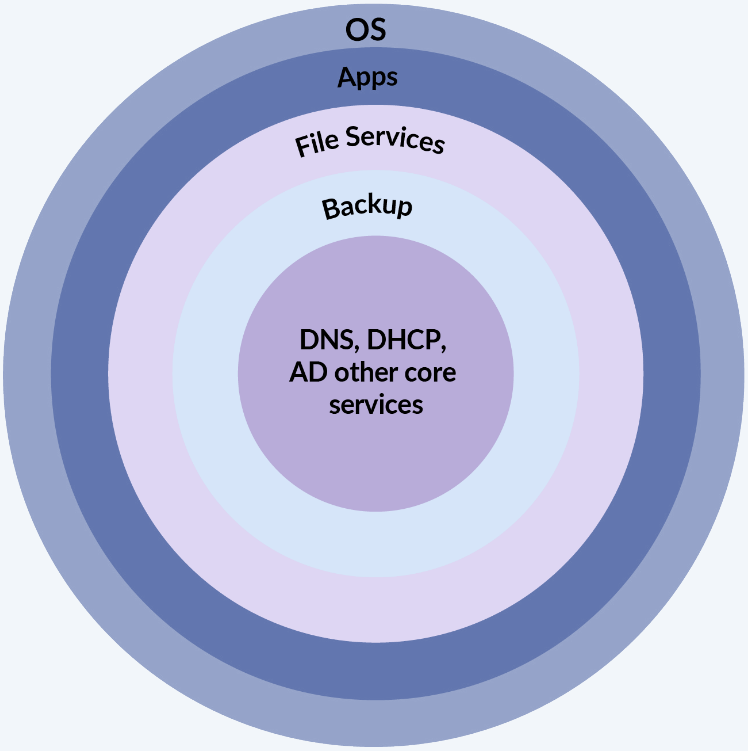
THE MSP RESPONSE

When disaster strikes, the hardest question to answer during the chaos of an active attack is where to start? Bringing your customer back online may require rebuilding from the ground up. The foundational services your business requires are domain name systems (DNS), dynamic host configuration protocol (DHCP), Active Directory (or other directory services), pre-boot execution environment (PXE), and other core services. You cannot talk about restoring backups until you can successfully log into servers which rely on these services.

Depending on the breadth of the spread of the ransomware, bringing your customers core services back online may be extremely difficult. There are many inter-service dependencies as well that may complicate the recovery effort. For example, Active Directory relies on DNS to find other domain controllers as well as the ability for clients to look up directory services. If servers are configured to use DHCP reservations, then you may have to physically assign IP addresses to hosts before you can begin. If you can get to the core servers, the worry might be, did your customer data get encrypted? To guarantee the threat is eliminated you may need to manually reinstall systems before core services can be recreated and enabled.

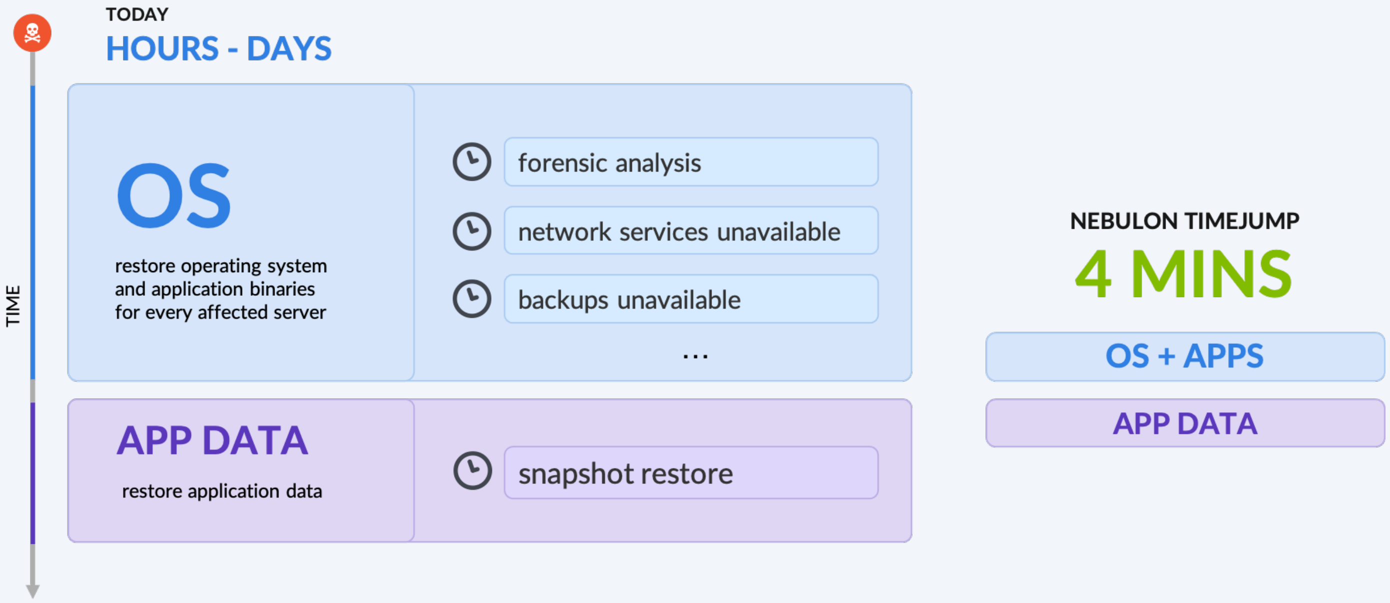
In catastrophic circumstances, your customer may be tempted to pay the ransom. However, many cyber insurance companies require that they be the ones to negotiate a payment, which will lead to delays and additional downtime for your customer. It's also important to note that making a ransom payment may result in your customer's organization being placed on a "whitelist" thus creating a soft target for follow up ransom demands.

This is where MSPs that include Nebulon TimeJump™ as a key component of a managed security practice can provide significant benefits to their customers as they work to recover the environment. TimeJump enables MSPs to restore entire infrastructure clusters to a previous state in under four minutes. If your customers core services are hosted on Nebulon nPods, you can simply roll the cluster back to a state prior to the incident. This



Core Enterprise Services

restores the core network services quickly so you can work on restoring backups (if required) and bringing customer applications back online. This can shorten recovery times from days (or even weeks) to minutes or hours. The ability to iterate over multiple snapshots for recovery until you discover the one right before the attack makes recovery quick and easy, adding immeasurable value to your MSP brand. This is not easily done with traditional recovery methods, especially in the case of operating system volume recovery (see image below.)



How TimeJump Works to Enhance MSP Managed Solutions

TimeJump leverages Nebulon immutable snapshots to create views of the cluster at a particular point in time as determined by a snapshot schedule. At the specified interval, the cluster will take a snapshot of every volume in the cluster, including the boot volumes. Each snapshot then becomes a candidate restore point for TimeJump. With sophisticated data reduction techniques, snapshots can be created frequently with minimal capacity overhead, providing you with many options for lowering the recovery point objectives for your customers.

When TimeJump is invoked, it takes a new set of snapshots for all volumes that can be used for forensic or insurance purposes. Then the cluster blocks host I/O to all volumes and restores the volumes to their original state from the restore point, including the host operating system root filesystem. The servers are automatically rebooted to allow them to boot from the restored volumes. This action restores both the server operating systems as well as their application data volumes. This process can take as little as four minutes to complete.

By restoring the complete state of the cluster to a time before the incident, recovery of the core infrastructure is much faster than would otherwise be possible. Quickly bringing up core services allows your MSP critical response teams to focus on getting applications and services back into production as soon as possible.

HOW MSPS GET STARTED WITH NEBULON TIMEJUMP

There are a few prerequisites that MSPs need to consider when setting up an nPod to successfully leverage TimeJump:

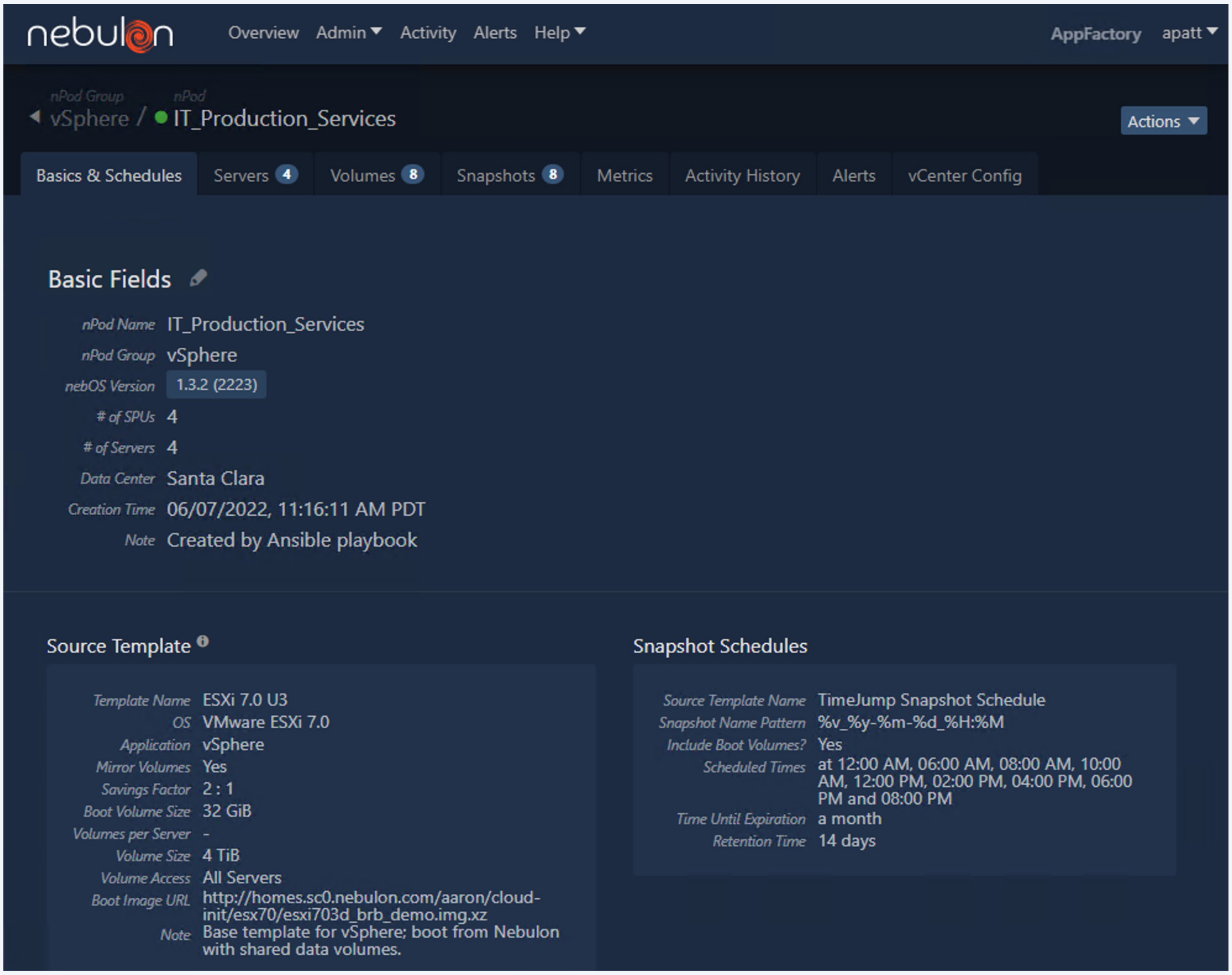
- □ The nPod must be running NebOS 1.3.2 or later.
- □ The nPod must have a snapshot template enabled which regularly takes snapshots of all nPod volumes, including the boot volumes.
- □ Lights out management (LOM) credentials should be configured for the nPod. While not a requirement, it will help automate the recovery process by automatically rebooting the servers.

Snapshot Templates

To create a compatible snapshot template, log into Nebulon ON, available at https://on.nebulon.com, and navigate to **Admin > nPod Management > Snapshot Templates** and then click the **Create** button. In the **Create Snapshot Template** screen, specify the following values:

Name	Enter a meaningful name for the snapshot template.
Snapshot Name Pattern	Name pattern for volume snapshots which uses the volume name + timestamp for naming. Leave at default values unless you require specific naming conventions.
Set snapshot expiration period	If checked, snapshots will be deleted after the specified period of time has elapsed. This determines how far back in time you can restore the nPod.
Set snapshot retention period	If checked, it prevents snapshots from being deleted for the specified amount of time.
Include Boot Volumes	If checked, creates snapshots of the server OS volumes as well as the data volumes. **This is required in order for TimeJump to work**.
Schedule	Schedule for how often to take snapshots. Nebulon recommends hourly snapshots.

Once you have created a snapshot template, you can attach it to your existing nPod by navigating to **Admin > nPod Management > nPods > {nPod name} > Basics & Schedules** tab. From there, click the **Actions** button and select **Add Snapshot Schedule**. Select the schedule you created to attach it to the nPod. Now the nPod will automatically create valid recovery points according to the schedule.



Basic Fields

nPod Name	IT_Production_Services
nPod Group	vSphere
nebOS Version	1.3.2 (2223)
# of SPUs	4
# of Servers	4
Data Center	Santa Clara
Creation Time	06/07/2022, 11:16:11 AM PDT
Note	Created by Ansible playbook

Source Template

Template Name	ESXi 7.0 U3
OS	VMware ESXi 7.0
Application	vSphere
Mirror Volumes	Yes
Savings Factor	2 : 1
Boot Volume Size	32 GiB
Volumes per Server	-
Volume Size	4 TiB
Volume Access	All Servers
Boot Image URL	http://homes.sc0.nebulon.com/aaron/cloud-init/esx70/esxi703d_brb_demo.img.xz
Note	Base template for vSphere; boot from Nebulon with shared data volumes.

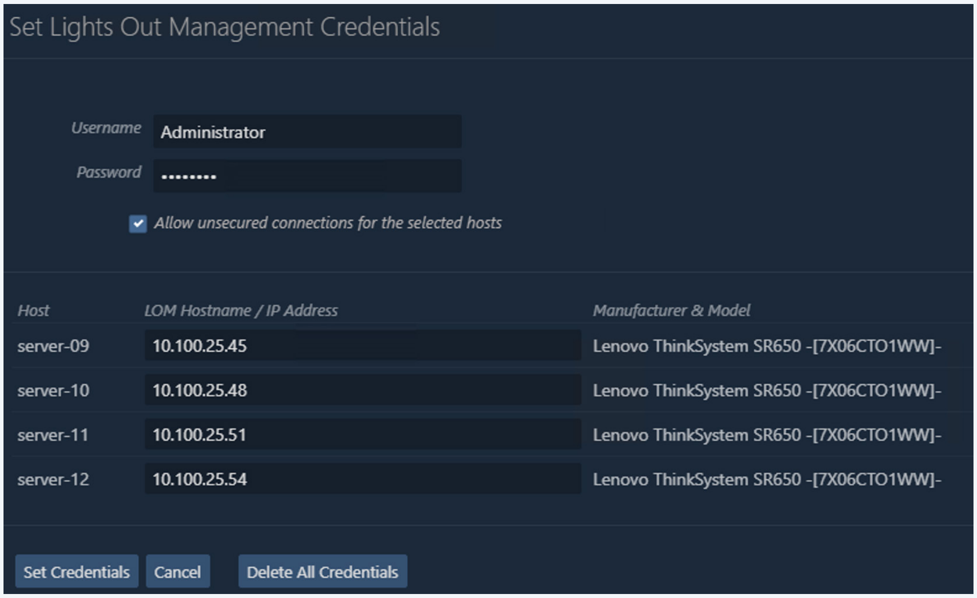
Snapshot Schedules

Source Template Name	TimeJump Snapshot Schedule
Snapshot Name Pattern	%v_%y-%m-%d_%H:%M
Include Boot Volumes?	Yes
Scheduled Times	at 12:00 AM, 06:00 AM, 08:00 AM, 10:00 AM, 12:00 PM, 02:00 PM, 04:00 PM, 06:00 PM and 08:00 PM
Time Until Expiration	a month
Retention Time	14 days

LOM INTEGRATION

Lights out management (LOM) integration allows Nebulon ON to automatically reboot servers as part of the TimeJump workflow. It also allows reporting of basic server telemetry in Nebulon ON, including system health. To configure LOM integration, navigate to **Admin > Physical Infrastructure**. From here, select the servers to configure LOM integration on and then click the [...] button and select **Set LOM Credentials**.

In the **Set Lights Out Management Credentials** page, set the username, password and address for the LOM controllers for each server. It is highly recommended you use IP addresses to remove dependencies on DNS which may be compromised during an incident.



Set Lights Out Management Credentials

Username: Administrator

Password: ....

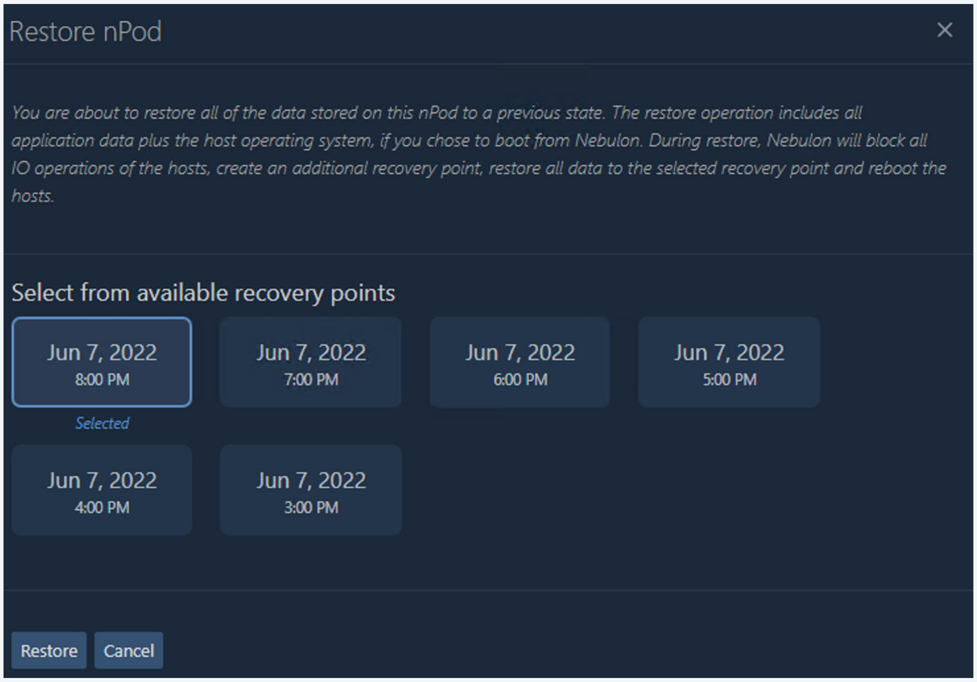
☑ *Allow unsecured connections for the selected hosts*

Host	*LOM Hostname / IP Address*	*Manufacturer & Model*
server-09	10.100.25.45	Lenovo ThinkSystem SR650 -[7X06CTO1WW]-
server-10	10.100.25.48	Lenovo ThinkSystem SR650 -[7X06CTO1WW]-
server-11	10.100.25.51	Lenovo ThinkSystem SR650 -[7X06CTO1WW]-
server-12	10.100.25.54	Lenovo ThinkSystem SR650 -[7X06CTO1WW]-

RESTORING A NPOD

To restore a nPod using TimeJump, log into Nebulon ON and navigate to **Admin > nPod Management** and select the nPod to be restored. From the **Basics and Schedules** tab, click the **Actions** button and select **Restore nPod**.

In the **Restore nPod** screen, select an available recovery point and click the **Restore** button.



Restore nPod

You are about to restore all of the data stored on this nPod to a previous state. The restore operation includes all application data plus the host operating system, if you chose to boot from Nebulon. During restore, Nebulon will block all IO operations of the hosts, create an additional recovery point, restore all data to the selected recovery point and reboot the hosts.

Select from available recovery points

Jun 7, 2022 8:00 PM — *Selected*

Jun 7, 2022 7:00 PM

Jun 7, 2022 6:00 PM

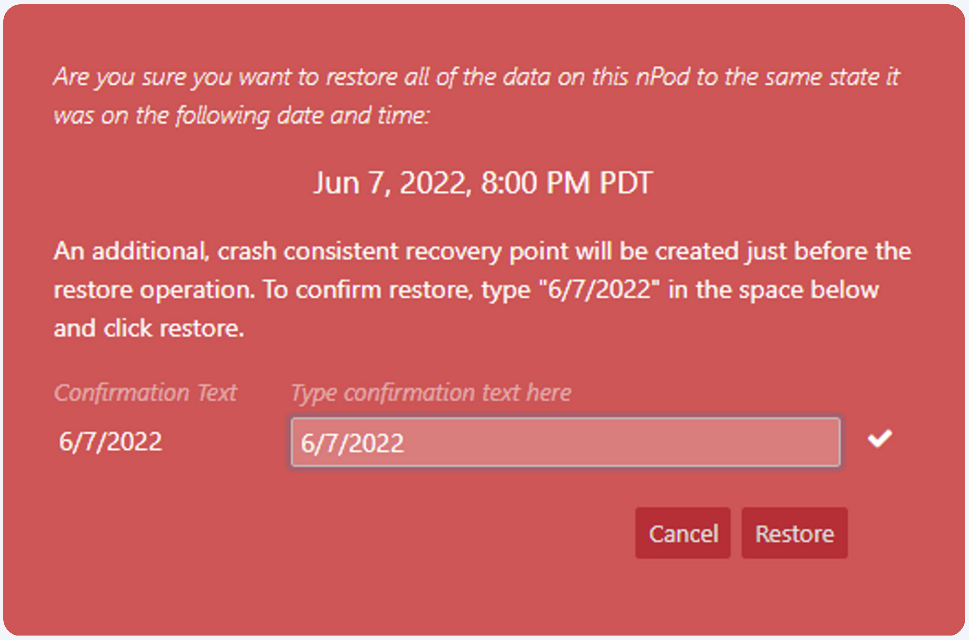
Jun 7, 2022 5:00 PM

Jun 7, 2022 4:00 PM

Jun 7, 2022 3:00 PM

NOTE: If you do not see any recovery points, your customers nPod does not have any valid snapshots to use for recovery points.

A warning will be presented indicating this action will revert the entire nPod and all of its data to the selected recovery point. You will need to type in the date to confirm the action. You can then press the **Restore** button to start the process of restoring the nPod.



Are you sure you want to restore all of the data on this nPod to the same state it was on the following date and time:

Jun 7, 2022, 8:00 PM PDT

An additional, crash consistent recovery point will be created just before the restore operation. To confirm restore, type "6/7/2022" in the space below and click restore.

Confirmation Text 6/7/2022

Type confirmation text here 6/7/2022 ✓

During the restore, all volumes in the nPod will be reverted to their exact state when the snapshot was taken, the servers will then automatically reboot, and the recovery is complete.

CHANCE FAVORS THE PREPARED

The pragmatic view is that preparing for a ransomware attack is preparing for the inevitable. To best position your customers to recover quickly in the event of a catastrophic incident there are some decisions you can make today that will set you and your managed services up for success.

Static Addressing

For well-known services and devices that will not change their IP addresses, consider assigning static IPs instead of relying on DHCP. Even if your customer is configured to use DHCP reservations, those clients may lose their IP addresses which will make recovery more complex. To aid in nPod recovery the Nebulon SPUs and the server LOM addresses should all be statically defined.

DNS

"It's always DNS" as the saying goes. The Nebulon SPUs will need to be able to resolve the public IP address for the Nebulon ON services during recovery. To help facilitate this, when configuring the IP addresses for the Nebulon SPUs, consider applying a public DNS server address as the secondary entry. This will preserve functionality if your customers DNS server was taken down in the incident.

Also, consider using IP addresses instead of fully qualified domain names (FQDNs) when configuring services that will not change in the normal course of doing business to further reduce the dependency on DNS.

Snapshot Schedule

The granularity and time horizon available to your customer for TimeJump recovery is directly tied to the distribution of snapshots. Craft a schedule that creates an acceptable Recovery Point Objective (RPO). If much of your customers core infrastructure changes slowly, perhaps a snapshot a day is sufficient. If things are more dynamic, increase the frequency you take snapshots. Remember to set sensible retention periods to avoid accidentally deleting recovery points.

NOTE: Snapshot retention protects the snapshots from being deleted, even by administrators.

Backup

Protecting your customer's backup solution is paramount to ensuring the best possible outcome when recovering from a ransomware attack. Follow the guidance of your preferred backup vendor to secure your customer's backup infrastructure. Regardless of the vendor, backup archives should be encrypted and available only to the backup application (i.e., do not place backup data on a network share). It is also advisable to create and maintain an offsite or offline backup.

For extra protection you can also host your customer's backup application on a Nebulon nPod and protect it with TimeJump along with the other core IT services. This ensures you have everything you need to make a quick and complete recovery for your customer.

Hypervisors

Follow the guidance for the deployed hypervisor vendor on securing the platform. This extends to the guest operating systems running on top of the platform as well.

- VMware – *Security Best Practices and Resources* – https://docs.vmware.com
- Hyper-V – *Plan for Hyper-V Security in Windows Server* – https://docs.microsoft.com
- Red Hat – *Securing Red Hat Enterprise Linux* – https://access.redhat.com

End Point Devices

If possible, secure network endpoint devices with an endpoint protection solution. Work with your other vendors to keep devices up to date with critical security patches. Some ransomware attacks are driven by compromised network devices that are incapable of running anti-malware or antivirus software so extra care should be taken to secure them.

Cyber Risk Insurance

Take time to understand the options available to your customers when shopping for cyber insurance. As ransomware becomes more prolific, rates to insure are increasing while the sub-limits for ransomware recovery costs are shrinking[4]. Use the terms of your customer's insurance to help shape your recovery plan and understand the details of your coverage. The forensic snapshots created when recovering your customer's nPod can be used to provide an audit trail to your insurance provider. Details on how to export snapshots can be found at https://on.nebulon.com/docs.

[4] GB&A – Ransomware Insurance: What to Look For

Training

According to the Verizon 2022 DBIR, 82% of data breaches involved the human element, generally through social engineering, phishing and other human focused attacks. Make training an important component of a ransomware strategy that your customer's organization makes an internal focused priority.

General Guidance

To wrap up, the Verizon 2022 DBIR gives the following general guidance on how to avoid becoming a target.

- □ Use two-factor authentication
- □ Do not reuse or share passwords
- □ Use a password keeper/generator app
- □ Be sure to change the default credentials of the point-of-sale (POS) controller or other hardware/software
- □ Ensure that you install software updates promptly so that vulnerabilities can be patched
- □ Work with your vendors to be sure that your customers infrastructure is as secure as it can be, and that they are following these same basic guidelines
- □ Keep a consistent schedule regarding backups and be sure to maintain offline backups
- □ Ensure that the built-in firewall is switched on for user devices such as laptops and desktops
- □ Use antivirus software for all your devices.
- □ Do not click on anything in an unsolicited email or text message
- □ Set up an out-of-band method for verifying unusual requests for data or payments
- □ Make sure the computer used for financial transactions is not used for other purposes such as social media or email
- □ Use email services that incorporate phishing and pretexting defenses
- □ Integrate Nebulon into any proactive customer ransomware recovery solution

nebulon.com

nebulon®