Service Description

Nexetic Backup for Microsoft 365

11.12.2023

Nexetic Oy

Tommi Tanttu

1. Introduction

1.1 Understanding the need for Nexetic Backup for Microsoft 365

Nexetic Backup for Microsoft 365 is a cutting-edge solution tailored to shield and back up data from customers' Microsoft 365 environments. As an increasing number of businesses make the transition towards cloud-based platforms, the importance of data protection has skyrocketed.

The necessity for M365 backup is rooted in the shared responsibility model between Microsoft and its M365 customers. While Microsoft ensures platform availability, customers bear the responsibility for data management and protection. Data loss in the cloud, contrary to common belief, is prevalent. Most often, these losses stem from user errors; however, emerging threats, like ransomware, also pose significant risks.

Recognizing these challenges, Nexetic offers a resilient backup solution to ensure that businesses never have to face the repercussions of lost crucial data.

1.2 About Nexetic

Nexetic is a renowned technology company committed to delivering state-of-the-art software solutions. With a focus on innovation, resilience, and customer-centricity, Nexetic has embarked on a journey to offer a premier backup solution for Microsoft 365, ensuring businesses always have access to their critical data.

1.3 Software-as-a-Service (SaaS) Model

The Nexetic Backup for Microsoft 365 is offered as a Software-as-a-Service (SaaS) model, which means customers can access the service over the Internet without needing to maintain the underlying infrastructure or software updates. This SaaS

model not only provides ease of use but also ensures that customers always have the latest features and security updates without the need for manual interventions.

1.4 Production Environment and Infrastructure

In our commitment to provide the best to our clients, the production environment for Nexetic Backup for Microsoft 365 is hosted on Microsoft Azure, one of the world's leading cloud platforms. Azure offers a plethora of benefits including, but not limited to, high availability, security, and extensive scalability options.

Nexetic leverages a serverless architecture built on top of Azure Services. This means the system can scale dynamically based on the workload, ensuring optimal performance without the overhead of managing server infrastructure. By eliminating the need for server provisioning, maintenance, and updates, Nexetic can focus on delivering a seamless experience to its users.

1.5 Scalability and Security

Being built on a serverless model atop Azure Services, the software can handle varying loads, catering to both small businesses and large enterprises with equal finesse. This elasticity ensures that as your business grows, Nexetic Backup for Microsoft 365 grows with you.

In addition to scaling, Microsoft Azure provides robust security features, ensuring that your data remains protected against threats. Combined with Nexetic's security protocols and best practices, customers can be assured that their data is in safe hands.

2. Integration with Microsoft 365

2.1 Introduction

The core value of Nexetic Backup for Microsoft 365 is its seamless integration with Microsoft 365. By tapping into Microsoft's ecosystem, Nexetic ensures that data backup and recovery are efficient, consistent, and secure. This chapter sheds light on the intricacies of this integration, the technologies used, and the authentication methods employed.

2.2 Microsoft Graph API

Microsoft Graph API is the gateway to data in the Microsoft 365 ecosystem. It offers a unified programmability model that Nexetic uses to access and interact with data in Microsoft 365, drawing from various services such as Outlook, OneDrive, SharePoint, and more.

Benefits of Using Graph API:

- Unified Access: Instead of using different endpoints or APIs for various Microsoft 365 services, Graph API offers a single access point, simplifying integration.
- Real-time Data Access: Changes or updates in the Microsoft 365 environment are immediately reflected and accessible, ensuring backups are always up-to-date.
- Granular Control: Nexetic can pinpoint specific data types, users, or services within Microsoft 365, allowing for flexible and tailored backup strategies.

2.3 Data Retrieval and Recovery

Using Graph API, Nexetic Backup for Microsoft 365 performs two main operations:

Data Retrieval: Nexetic taps into the Microsoft 365 environment to fetch the latest data. This data is then securely transferred and stored in the Nexetic infrastructure, ensuring that backups are always current.

Data Recovery: In case of data loss or corruption within Microsoft 365, Nexetic uses Graph API to restore the backed-up data back into the respective Microsoft 365 service. This ensures swift recovery with minimal disruption.

A serverless worker in our Azure tenant is responsible for periodically downloading data from the customer M365 tenant to our cloud. It uses use official Graph API SDK for .NET with HTTPS and TLS1.2. That ensures encryption of data in transit and authority of the source. A bearer oauth2 token is generated for the operation and is used to do the queries against the API. The token is valid for 1 hour. The metadata is saved to a cloud SQL database and content is sent to blob storage, both in Nexetic Azure tenant.

2.4. Authentication Mechanism

Nexetic understands the criticality of data security and privacy. Therefore, a robust and secure authentication mechanism is employed when integrating with Microsoft 365.

Customers sign in using Microsoft's Single Sign-On (SSO) authentication, which boasts advanced multi-factor authentication (MFA) capabilities. For enhanced reliability, there's also an option to set up an independent login/password combination. This serves as a robust alternative for access in the event of any downtime with Microsoft SSO.

Microsoft SSO uses OAuth 2.0, an industry-standard protocol for authorization, logging users into the backup portal. This protocol allows third-party applications like Nexetic to access user profile data without exposing the user's password.

2.5. Initial Permission Granting

To initiate the functionality of the Nexetic Backup application, permissions need to be explicitly set. The sole authority to grant these permissions lies with the **Global Administrator** within Microsoft 365. This action is a singular requirement, necessary before any backup operations can commence. The permissions can be later managed in Azure and granularly revoked if some of them become obsolete. Even after the initial setup, the customer is always in control of what data Nexetic can access.

Admin consent:

API Name	Claim value	Permission	Type
Microsoft Graph			
Microsoft Graph	profile	View users' basic profile	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated
Microsoft Graph	Group.Read.All	Read all groups	Delegated
Microsoft Graph	openid	Sign users in	Delegated
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated
Microsoft Graph	Mail.ReadWrite	Read and write mail in all mailboxes	Application
Microsoft Graph	OrgContact.Read.All	Read organizational contacts	Application
Microsoft Graph	User.ReadWrite.All	Read and write all users' full profiles	Application
Microsoft Graph	Mail.ReadBasic.All	Read basic mail in all mailboxes	Application
Microsoft Graph	Group.Read.All	Read all groups	Application
Microsoft Graph	Directory.ReadWrite.All	Read and write directory data	Application
Microsoft Graph	MailboxSettings.Read	Read all user mailbox settings	Application
Microsoft Graph	Sites.Read.All	Read items in all site collections	Application
Microsoft Graph	Sites.ReadWrite.All	Read and write items in all site collections	Application
Microsoft Graph	Contacts.ReadWrite	Read and write contacts in all mailboxes	Application
Microsoft Graph	Sites.Manage.All	Create, edit, and delete items and lists in all site collections	Application
Microsoft Graph	Files.ReadWrite.All	Read and write files in all site collections	Application
Microsoft Graph	User.Read.All	Read all users' full profiles	Application
Microsoft Graph	Files.Read.All	Read files in all site collections	Application
Microsoft Graph	Mail.Read	Read mail in all mailboxes	Application
Microsoft Graph	Calendars.ReadWrite	Read and write calendars in all mailboxes	Application
Microsoft Graph	MailboxSettings.ReadWrite	Read and write all user mailbox settings	Application
Microsoft Graph	Contacts.Read	Read contacts in all mailboxes	Application
Microsoft Graph	Mail.ReadBasic	Read basic mail in all mailboxes	Application
Microsoft Graph	Application.Read.All	Read all applications	Application
Office 365 Exchange Online			
Office 365 Exchange Online	User.Read.All	Read all users' full profiles	Application
Office 365 Exchange Online	full_access_as_app	Use Exchange Web Services with full access to all mailboxes	Application
Office 365 Exchange Online	Mail.ReadWrite	Read and write mail in all mailboxes	Application
Office 365 Exchange Online	User.ReadBasic.All	Read all users' basic profiles	Application
Office 365 Exchange Online	Mail.Read	Read mail in all mailboxes	Application

User consent (For all users accessing the backup portal):

API Name	Claim value	Permission	Type
Microsoft Graph			
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	openid	Sign users in	Delegated
Microsoft Graph	profile	View users' basic profile	Delegated
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated

2.6. Defining Backup Administrator Roles in Nexetic

Within the Nexetic Backup system, users designated as backup administrators must align with one of these specific roles from the Microsoft 365 ecosystem:

Global Administrator
Exchange Administrator
SharePoint Administrator

These roles ensure comprehensive access to perform backup operations effectively across the platform.

2.7. Limited Access for Other Roles

While users outside of the above-stated roles can access the Nexetic Backup portal, their visibility and control are restricted.

They are limited to viewing and managing only their individual data within Exchange and OneDrive, ensuring personalized data access. Broad backup or administrative functionalities remain beyond their purview.

3. Data Security and Compliance

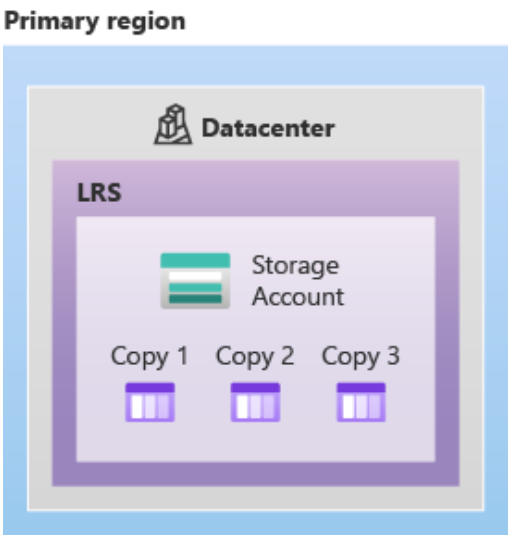
3.1. Data storage

3.1.1. Azure

The service is offered from Microsoft Azure's North Europe data center, which has the following certificates: CDSA, PCI DSS, Shared Assessments, TruSight, EBA, EN 301 549, ENISA IAF, GDPR, EU Model Clauses 2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001 PCI DSS, SOC, WCAG, EBA, EN 301 549, ENISA IAF, GDPR, EU Model Clauses. The data center is located in Ireland.

The customer's data is saved to Azure blob storage. Azure blob storage uses Azure Storage Service Encryption (SSE) to automatically encrypt data at rest. When the data is prepared for a restore/download operation it is decrypted. The encryption and decryption are transparent to the user. The encryption uses 256-bit AES encryption, which is one of the strongest block ciphers available. Each customer's data is stored in individual buckets within storage, ensuring segregation and data integrity.

By default, the storage strategy utilized is Locally Redundant Storage (LRS). This is a replication method provided by the Azure platform, crafted to maintain data availability and durability within the primary region by mirroring it across several



devices.

- Triple Replication: LRS replicates your storage account data three times, but all within a single data center in the primary region. This provides resilience against local hardware failures.
- High Durability: With LRS, the durability of objects over a given year is guaranteed to be at least 99.999999999% (often referred to as "11 nines").
- Cost-Efficient: Among the various redundancy options offered by Azure, LRS is the most cost-effective. However, it is essential to note that while it offers significant durability within its scope, its durability is lesser in comparison to other redundancy options.
- Protection Scope: LRS primarily safeguards your data against issues like server rack failures or drive malfunctions within the data center.
- Synchronous Writes: When a write request is made to a storage account utilizing LRS, the operation is synchronous. This means the write operation is only deemed successful after data has been written to all three replicas, ensuring data integrity. The data saved to Azure blob storage is replicated to three disks which protects it against drive and server rack failure.

3.1.2. Nexetic Cloud Storage Finland

The data center is hosted at Verne Global Finland's high security bunker in Finland. Verne Global Finland has received multiple Green Data Center certifications such as PAS2060 Climate Neutral Company and CICERO Dark Green rating.

Verne Global Finland security certificates:

- ISO 27001
- ISO 22301
- PCI DSS
- Katakri (Finnish National Security)

Storage backend is implemented with Ceph. Ceph is an industry standard scalable sharded shared-nothing distributed storage. The architecture doesn't have any bottlenecks or centralized points of failure.
The internal networks are built on industry standard principles of redundancy and are mostly running on high-speed 100Gbit/s links.

The service layer is built on top of a VMware vSphere cluster running on dedicated high-performance servers.

Our Industry standard Ceph data lake installation uses a mix of HDD and NVMe drives. Most of the data resides on HDD, while all metadata is on NVMe drives making data access fast and latency small.

Ceph redundancy is optimized for available space with no sacrifice in redundancy. By default it will handle up to 2 simultaneous hardware failures at disk or server level without any downtime or data loss.

Ceph is trusted and developed by major industry players such as Intel, Red Hat, DigitalOcean, Cisco and Canonical. It is a topic of active research by CERN and University of Kentucky among others. Ceph is used in most HPC (High Performance Computing) clusters around the world, such as the European joint HPC venture LUMI.

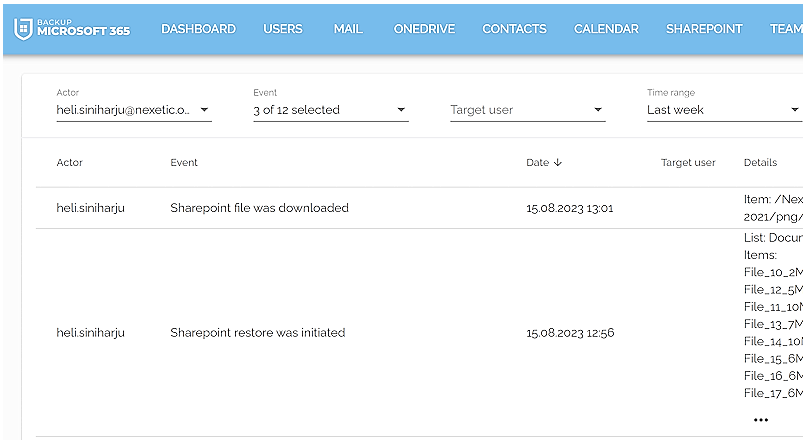
Data is encrypted with AES 256bit. Encryption is done in storage server. Data transit from Azure to storage is encrypted with TLS connection.

Each customer's data is stored in individual buckets within storage, ensuring segregation and data integrity.

When using this storage, metadata remains in Azure, ensuring consistency and security.

Layered Security Model: Top-of-the-line firewall infrastructure, intrusion detection, and isolated network zones.

3.2. Audit Log



Administrators can access the Audit Log where they can get in-depth insights into every backup-related action. They can utilize advanced search features to swiftly pinpoint user activities, capturing the 'who, what, and when' within the backup portal.

3.3. Additional Documentation

Additional information: Nexetic Support pages at https://support.nexetic.com/ -> Nexetic Backup for Microsoft 365