VERITAS

Veritas Alta View

Security and operations overview.

White Paper | March 2023

VERITAS ALTA™

Introduction

Veritas Alta™ View is a centralized management service for the entire data protection estate. It provides a single user interface (UI) to drive simplicity for managing multiple NetBackup™ domains, whether deployed on-premises or in the cloud. Management options include various management functions for the Veritas NetBackup software within each NetBackup domain. This eliminates the need to use multiple dedicated UIs to manage backup jobs, policies, and other features included within Veritas Alta View. Veritas Alta View also provides a single point of access to additional Veritas Alta™ cloud-based services, such as Veritas Alta™ Backup as a Service.

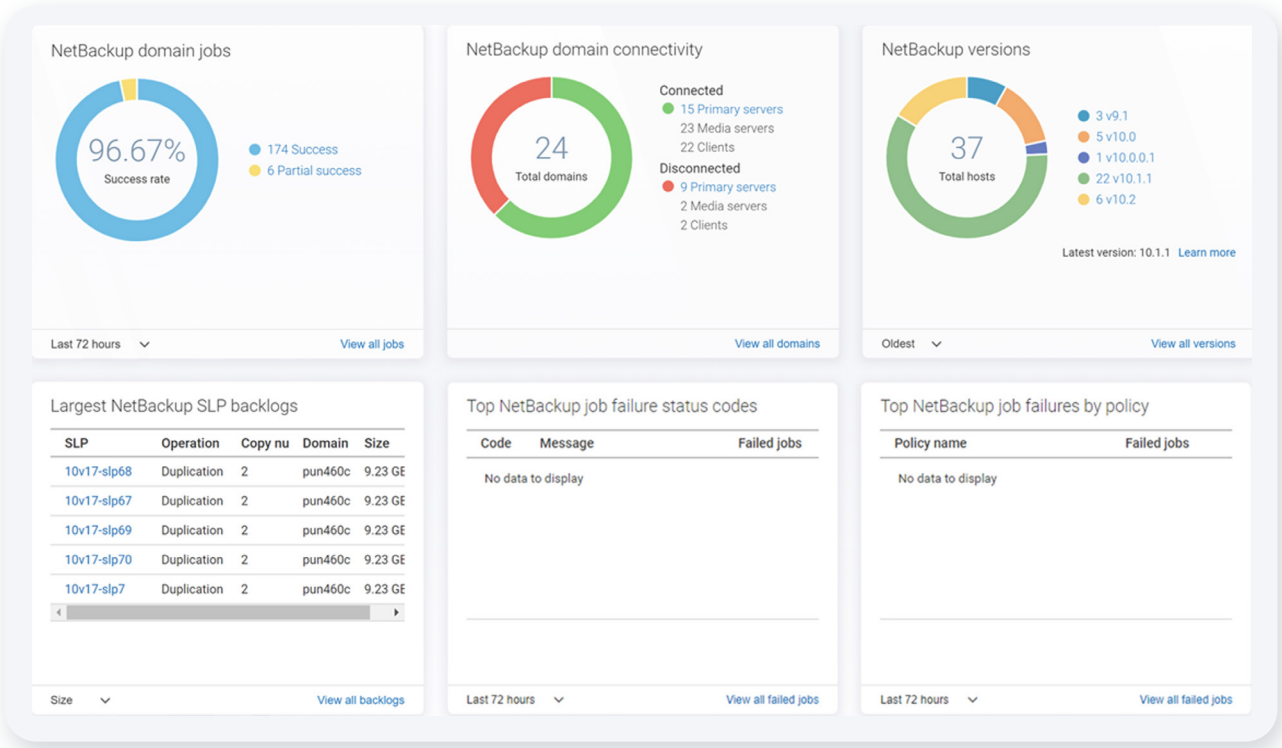


Figure 1. Veritas Alta View dashboard example

Connection from NetBackup to Veritas Alta View

NetBackup primary servers connect to Veritas Alta View and Veritas Alta™ Analytics endpoints to send metadata such as policy and job details, and also to get API calls from Veritas Alta View to perform management tasks such as changing policies.

The NetBackup primary server uses two means of communication: Veritas Alta™ Data Collector and NetBackup WebSocket client. Veritas Alta Data Collector and NetBackup WebSocket are installed on the primary server. All connections to Veritas Alta View and Veritas Alta Analytics are outbound-initiated on port 443 (HTTPS).

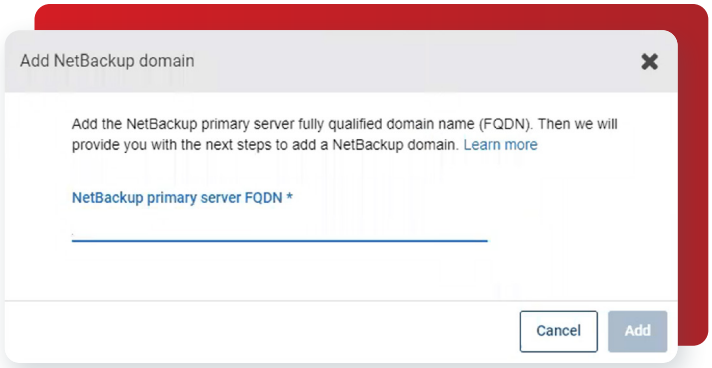


Figure 2: Add a NetBackup primary server dialouge box

Veritas Alta Data Collector sends data to Veritas Alta Analytics which is used by Veritas Alta View, and the NetBackup WebSocket client sends data directly to Veritas Alta View.

Connecting a primary server to Veritas Alta View requires a registration file to be downloaded from Veritas Alta View. This registration process sets up a secure means of bi-directional communication between NetBackup and Veritas Alta View.

The registration file is customized for each NetBackup primary server; it includes an API key and the public certificate from Veritas Alta View. The API key is unique to each NetBackup primary, and used by Veritas Alta View to authenticate connections and requests. The public certificate is used to ensure that NetBackup can only connect to the Veritas Alta View endpoint and none other.

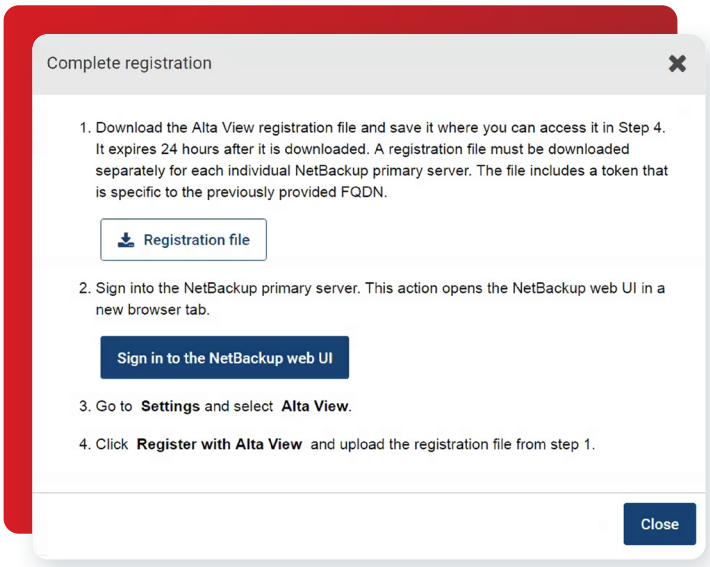


Figure 2: Add a NetBackup primary server dialouge box

The registration file must be installed on the specified primary server within 24 hours after it has been downloaded (see Figure 3). Authorization to install the registration file on the primary server is included in the administrator role of NetBackup. After the registration file is installed, the primary server will complete the registration process with Veritas Alta View.

Mutually, NetBackup creates an API key for Veritas Alta View automatically as part of registration, enabling bi-directional authorization. API keys are fully manageable and available to rotate.

As a final part of the registration process, Veritas Alta Data Collector consumes the registration file which has the information needed to connect the primary server to Veritas Alta Analytics. JSON web tokens are used for communication between Veritas Alta Data Collector and the NetBackup primary server.

Connection Details

All communication between the primary server and Veritas Alta View is secured with TLS 1.2 using the most secure cipher suites. The API key and token used for authorizing the connection are stored in encrypted format on the primary server.

The primary server needs to connect to two Veritas Alta endpoints on port 443:

- https://alta.us.veritas.com
  Used for a bi-directional WebSocket HTTPS connection.
- https://analyticsagent.us.veritas.com
  Used for a uni-directional HTTPS connection by the Veritas Alta Data Collector.

Use of a proxy is supported between NetBackup and Veritas Alta. Proxy configuration is supported for NetBackup versions 10.1.1 and newer. The Veritas Alta Data Collector only collects information necessary for operational capability and does not read backups or collect backup content data such as filenames or user information.

Veritas Alta View Customer Data Management

Veritas Alta View will communicate with one or more NetBackup Primary Servers to collect data in order to provide monitoring and management capabilities. Veritas Alta View stores metadata about the NetBackup environment. If a customer de-provisions, the Veritas Alta View data is removed within 30 days. The Veritas Alta Analytics metadata regarding image backups is stored indefinitely for compliance reporting reasons but transient metadata is deleted as it is deleted within NetBackup.

Our privacy policy and data handling procedures are documented on our website, with links included at the end of this document.

Data Security

Data Deletion

Data purges from Veritas Alta View happen periodically every seven days for job data; however, the data related to a specific domain can be deleted manually within Veritas Alta View. Data purges within Veritas Alta Analytics are configurable for several objects, but jobs data is stored indefinitely for compliance reporting reasons.

Secure Virtual Customer Domains

Every Veritas Alta View customer is provisioned a secure environment, where the boundaries are controlled to only allow the appropriate communication and keep undesired traffic out. Each customer is provisioned as a tenant within Veritas Alta View, which is the management plane and hosted in Azure, and within Veritas Alta Analytics which is hosted in Oracle Cloud Infrastructure. Veritas Alta View uses Azure Web Application Firewall. Veritas Alta Analytics uses Oracle's Web Application Firewall (WAF). Proxies are also supported.

Vulnerability Scanning

Veritas conducts regular vulnerability scanning using internal and third-party assessment of security, with penetration testing in pre-production and production. These periodic tests help ensure that Veritas Alta View remains secure.

Veritas uses standard industry processes and tools for assessment and notification of external threats and software vulnerabilities discovered by other trusted security sources.

Encryption

Encryption of data-in-transit is applied to communication across all cloud boundaries, including back to any on-prem NetBackup primary server. Encryption of data-at-rest within Veritas Alta View is done using AES-256. Encryption of data-at-rest within Veritas Alta Analytics is done with Oracle using transparent data encryption (TDE).

Encryption Key Management

Veritas manages key encryption keys for Veritas Alta View using Azure Key Vault. All customer metadata at rest is encrypted using keys derived from Azure Key Vault. All sensitive information within Veritas Alta Analytics is protected and encrypted with RSA keys. Veritas manages key encryption keys for Veritas Alta View control plane and data plane.

Application Security

The Veritas Application Security Assurance Program (ASAP) is a risk-based software assurance process that includes comprehensive and rigorous software development processes and procedures that are consistent with Building Security in Maturity Model (BSIMM) industry standards. The ASAP scrutinizes products across different categories. These categories include:

1) Training (application security specific);

2) Requirements (data classification);

3) Design (threat modeling and cryptography);

4) Implementation (static and dynamic analysis security testing);

5) Verification (vulnerability scan and third-party pen testing);

6) Deployment (third-party software review and readiness); and

7) Operations (customer support for security and vulnerability management).

Role-Based Access Controls

Role-based access control (RBAC) is built into each tenant, with zero trust between tenants, delivering a separation of duties within the product. The default role within Veritas Alta View is specific to the functions available within the product, and custom roles are available to limit permissions and access to specified NetBackup domains.

Identity Management

Customers can choose to integrate their own Identity Provider (IDP) with Veritas Alta View or use Veritas as the IDP. Veritas recommends that customers use their own IDP to better manage identity lifecycle and make use of existing controls from their IDP such as multi-factor authentication (MFA), conditional access policies and device checks, and more. Veritas offers its own IDP to help get started quickly (see Figure 4) with the ability to switch over to an external IDP at any point.

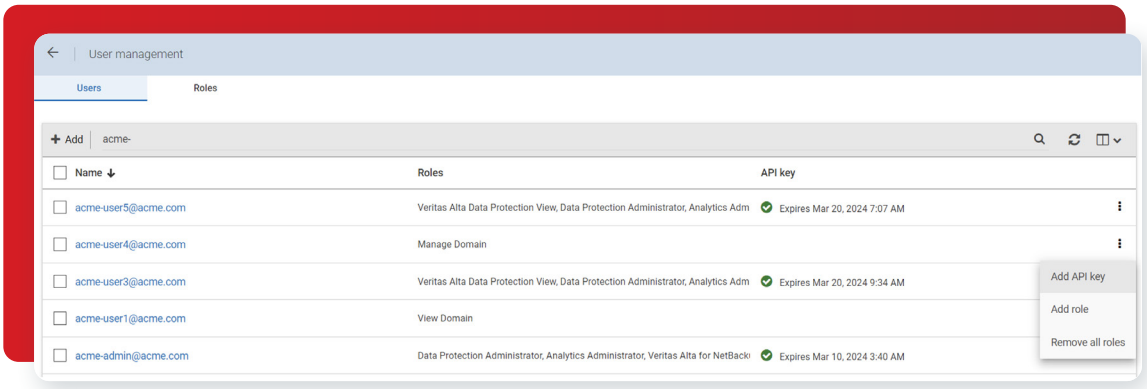


Figure 4. Veritas Alta View user management

The Veritas IDP works by creating user accounts based on user's organizational email address. Strong password policies with historical checks are enforced and enrollment for MFA is mandatory. The Veritas' IDP is powered by Okta Cloud which provides MFA options via mobile authenticator apps. Email and SMS factors are explicitly disabled since they are less secure.

Each user can additionally obtain an API key which allows programmatic access to the Veritas Alta View REST APIs in the context of that user and the roles they have been assigned.

Password Policy for the Veritas IDP

These restrictions apply only to user accounts created in the Veritas IDP:

- Minimum of eight characters in length
- No more than two identical characters in a row
- Must contain at least three of the following four types of characters
    - Special characters (!@#$%^&*)
    - Lower case (a-z)
    - Upper case (A-Z)
    - Numbers (0-9)
- Do not allow re-use of the previous 10 passwords
- Prevent use of passwords containing parts of a user's email address or name
- Do not allow passwords that are part of 10,000+ commonly used passwords

Attack Protection

Veritas enables various mechanisms to protect against user account attacks such as suspicious IP throttling and brute force protection.

Session Management

After users have authenticated, a session is created for them in Veritas Alta View. The session expires after 15 minutes of inactivity and has a hard limit of six hours; after six hours the user must re-authenticate. Shortly before reaching the inactivity limit and the session limit, users are informed within the web application that they will be logged out and have a choice to extend an inactive session or to re-authenticate there and then.

Sessions are controlled by Veritas Alta View and each user session ID is stored in a secure cookie on the browser for the duration of their session. The cookie is a temporary'*session* cookie which is deleted by the browser when it is closed.

User Auditing

All end-user logins, in-application activity and API client activity is audited (see Figure 5). Additionally, per data handling guidelines, all Veritas access to production resources (Support, Provisioning & Management, Security Operations Center) is also fully audited.

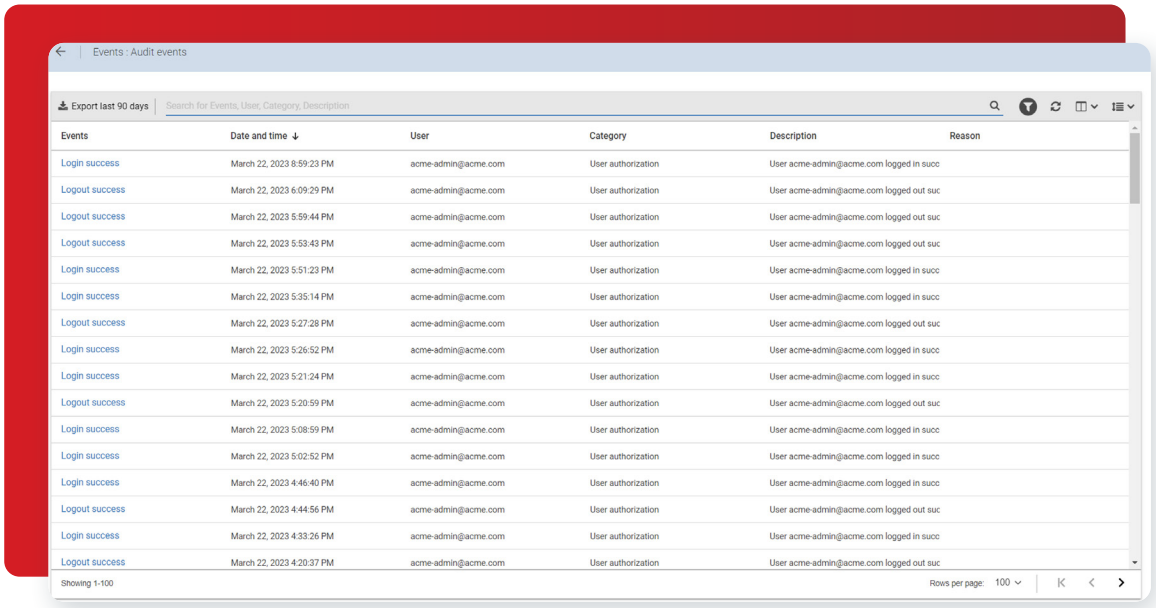


Figure 4. Veritas Alta View user management

Conclusion

Veritas Alta View is a secure SaaS application, built for the web while meeting the need to manage hybrid NetBackup domains in datacenters all over the world and within the cloud. Veritas is committed to the security of your data by following industry best practices. Rest assured safeguards are in place to help secure your data within the Veritas Alta portal, and communications in and out of Veritas Alta View. With these clear network communication requirements, you can easily add a domain to Veritas Alta View and increase operational simplicity and configuration management with a single UI.

Related Documentation

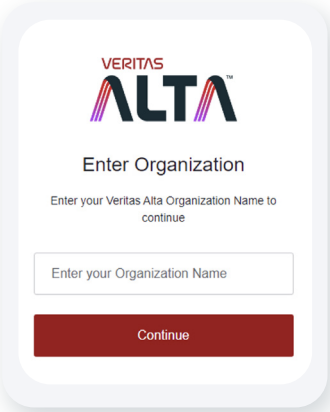
Veritas Privacy Policy:

veritas.com/company/privacy

Data Processing Terms and Conditions (GDPR)
veritas.com/content/dam/Veritas/docs/policies/Veritas%20Data%20Processing%20Terms%20and%20Conditions%20and%20new%20SCCs.pdf

Access Veritas Alta View here:

alta.us.veritas.com



About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1863 03/23