Ivanti Service Manager Cloud Security

White Paper

Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”) and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

1. Executive Summary

Security is one of the most important considerations when choosing a cloud partner. Ivanti takes security and data privacy obligations very seriously and implements best-in-class security and hosting practices.

Today's global, mobile workforce requires services that are always available and ubiquitous. This requires a level of availability and security practices that are often beyond most IT organizations. At Ivanti, security and data protection start at product inception and continue through a "security by design" model that includes security considerations in all phases of the product—from design and implementation through operations. Ivanti's security and hosting practices are better in design than most traditional on-premise implementations. Ivanti's best-in-class offerings include disaster recovery practices that are continually tested and audited by third parties to ensure compliance with industry standards. Ivanti maintains certifications such as ISO27001, SOC 2 Type II and FedRAMP.

This paper highlights Ivanti's approach to a comprehensive security model within the context of the cloud- optimized Ivanti® Service Manager solution, encompassing the people, the organization, development, operations, and independent third-party certifications.

2. Security Organization and Culture

2.1. Security Organization

Multiple layers of security are set in place within the Ivanti organization. Ivanti's Chief Security Officer (CSO) and Security Council are responsible for overall security communication, implementation, and response reporting to executive management. Ivanti's overall security organization includes a specialized focus on implementing and maintaining security best practices within the cloud services[1] provided. Ivanti's engineering and architecture teams provide independent, secure design reviews.

2.2. Background Checks

All Ivanti employees go through industry-standard background checks upon hire as permitted by local legislation to verify education, previous employment, and references.

2.3. Security Training

As part of Ivanti's ongoing security awareness training, all employees are required to complete security training upon hire and as well as on an ongoing basis. Subsequent to hire, Ivanti regularly trains all staff members with anti-phishing campaigns, annual acceptable use attestation, and Open Web Application Security Project (OWASP) Top 10 training for development. Ivanti also provides role-specific security training modules to employees.

[1] Cloud Services referenced in this whitepaper are specific to Ivanti Service Manager

3. Cloud Development Security

The development processes for Ivanti cloud products have a dedicated security focus and adhere to the principles in OWASP's Application Security Verification Standard (ASVS).

3.1. Design Reviews

Prior to and during implementation, architects trained in security best practices review designs to ensure developers adhere to security decisions on implementation. Ivanti follows best-practice models for the software development lifecycle. This process includes security training for Ivanti's architects, developers, QA, and support staff.

3.2. Security Testing

Security testing is part of the development cycle with the use of security scanners to identify vulnerabilities throughout the cycle. Ivanti uses industry-leading, third-party tools to test and validate secure implementation as well as reduce flaws. Ivanti closely monitors, responds to, and resolves potential security issues as defined by Ivanti's Computer Security Incident Response Plan (CSIRP). Ivanti employ a multi-tiered approach to ensure a comprehensive and secure development process.

4. Operations Security

4.1. Physical Security

To ensure the highest levels of compliance, redundancy, and fault tolerance, Ivanti uses best-in-class infrastructure with multiple vendors in geographically dispersed SOC2 TYPE II, ISO27001 and FedRAMP-compliant facilities. Ivanti leverages the security provided by its hosting providers, and additionally provides physical security access to its own sites. This includes a secure environment with established security controls to prevent, detect, and respond to vulnerabilities and data breaches. Ivanti also complies with local, state, federal, and international regulations regarding security, privacy and data handling, and use facilities required for ISO27001, FedRAMP, and SSAE 18 compliance.

4.2. Logical Security

Ivanti employs industry-wide best practice Defense-in-Depth strategy, placing multiple layers of defense throughout the cloud environment. Ivanti relies on security appliances from multiple vendors, at multiple layers of the OSI model.

(ISC)^2 CISSP® certified engineers actively monitor and manage security incidents in cloud security infrastructure. The engineers are available to address issues, including distributed denial-of-service attacks (DDoS), intrusion detection/prevention events (IDS/IPS), global correlation of events, source reputation, and Layer 7 Web Applications Firewalls (WAF). Ivanti maintains a 24x7x365 Security Operations Center (SOC) that monitors and responds to Security Information and Event Management (SIEM) incidents.

4.3. Transport Security

The ISM Cloud product transfers data securely through industry-standard methods such as HTTPS using TLS, AES 256-bit encryption, and 2048-bit certificates. Under special circumstances, Ivanti is also able to provide a VPN connection to support integration to solutions that are not able to communicate via the public internet or through web services. When configured, the VPN connections use industry-standard AES 256 IPsec encryption.

4.4. Authentication, Authorization, and Accounting (AAA)

Ivanti provides full AAA protection, while also offering customers several options to simplify the user login experience without compromising security. For instance, customers wishing to add enhanced single-sign-on capability may integrate existing security environments using several different authentication methods:

- Local Authentication (passwords are stored inside the ISM Cloud system and are maintained separately from network credentials)
- SAMLv2 (Security Assertion Markup Language) or Microsoft Active Directory Federated Services/ADFS are the most common methods of Authentication. SAML handles authentication completely for the user. The ISM Cloud system accepts “tokens” or “assertions” from the system as proof that the user is allowed access to the ISM Cloud system.
- LDAP/LDAPS (Secure LDAP) and StartTLS. LDAP authentication is an optional feature separate from the LDAP bulk-user-records import feature. LDAP authentication will collect the user’s username and password and then send a request to the user’s LDAP server. The LDAP server will respond to the ISM Cloud to allow or deny access. If the user’s LDAP server does not allow user access (wrong password or account disabled), ISM will not allow access either.
    - The two biggest advantages of this method are that it can provide SSO access to ISM Cloud without a user needing to enter a username and password. If a password is required, the interaction remains solely between the system and the user, thus not exposing login credentials outside of the corporate network. Ivanti recommends the use of SAML to integrate access to Ivanti’s Cloud environments with the user’s access provider.
- OpenID authentication allows you to utilize an existing account to sign in to multiple websites without creating new passwords. OpenID will collect the user’s name and password and then send the request to an authentication server which then sends the request to ISM Cloud to deny or allow access.
- OpenID Connect authentication allows users to verify their identity based on the authentication performed by an authorization server. OpenID Connect capabilities are integrated into the protocol and no extension is needed.

4.5. Data Privacy

Ivanti's Data Privacy Policy satisfies regulatory requirements and governs Ivanti Cloud information-handling practices. See this link to access the Ivanti Privacy Policy: https://www.ivanti.com/company/legal/privacy-policy.

Privacy laws and contract compliance prevent the use of customer data for any non-customer contractual processes. Ivanti staff members are not allowed to move customer data from a customer environment for the purposes of development, test, or research. Additionally, Ivanti's Data Classification and Handling Policy and Customer Data Transfer Standard require customer data to be classified and handled such that data is protected to a level commensurate with the sensitivity of the data.

4.5.1 Separate Tenant Databases

Securely housing customer data in separate databases ensures tenant data confidentiality. Additional application-specific controls protect data from unauthorized access across multiple layers of the application.

4.5.2 Encryption of Sensitive Data

Customers have an option to encrypt specific fields in the application such as Personally Identifiable Information (PII) or other sensitive data. For more information on how Ivanti Service Manager complies with GDPR, refer to https://rs.ivanti.com/downloads/ivanti-itsm-gdpr.pdf.

4.5.3 Data Access Controls and Auditing

The ISM Cloud environment has restricted access to customer data. Ivanti uses several layers of controls for monitoring, including administrative and technical controls. Customers can choose to authorize access to Ivanti Cloud Operations or Ivanti Support Services staff for testing or validation purposes.

4.5.4 Data Encryption in Transit

To secure data in transit, Ivanti supports TLS 1.1, 1.2, and 1.3. If the connecting browser uses the latest standard, it will default to the latest TLS version. Ivanti uses industry standard AES encryption strength 2048-bit certificates.

4.5.5 Data Encryption at Rest

To secure data at rest, Ivanti provides encryption for all data centers at no additional cost to customers. For this, Ivanti encrypts the volume with a data key using the industry-standard AES-256 algorithm.

4.5.6 ISM Cloud Storage Data and Privacy

Data stored in ISM Cloud will be stored until the customer requests its removal or until specified in the contracted agreement. To request removal of data, the customer simply sends a request to the assigned Ivanti representative. The data is stored in tenant-specific blob storage to ensure customer security and privacy.

No customer can access, view, or alter any data from any other customer. Teams are available to troubleshoot any issues that may arise with a customer, but Ivanti will not conduct any action without written approval from that customer. Audit trails are in place to record any actions performed on the customer's behalf, along with a traceable link of their express approval.

Ivanti does not store customer credentials in ISM Cloud. Customer credentials cannot be decrypted by Ivanti or anyone else. Customer data in ISM Cloud is stored by tenant, meaning that only that customer (tenant) can access the data.

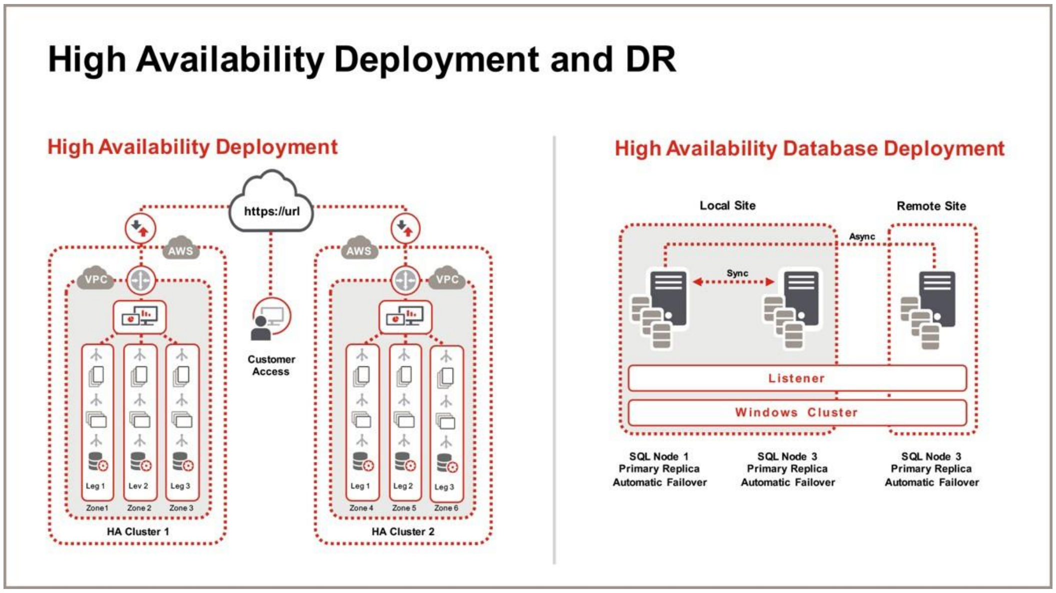
Anonymized data is applied to Data Science/Machine Learning for research purposes, to develop machine learning models and or peer data evaluation. Per the EULA, no customer Personally Identifiable Information (PII) will be shared with the data science team or any other customer.

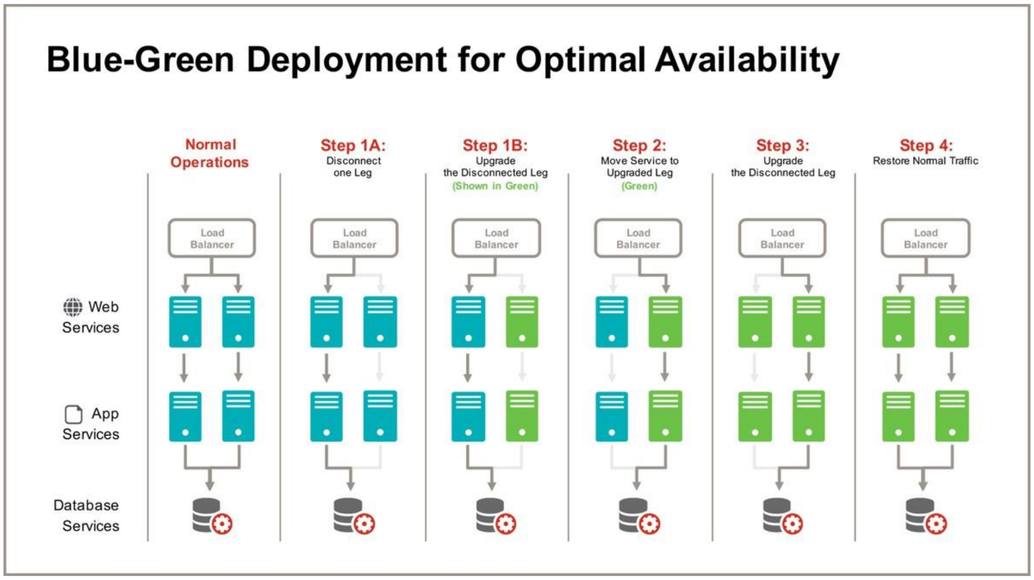
- Ivanti GDPR Documentation
  https://community.ivanti.com/docs/DOC-67844
- Ivanti Privacy Policy
  https://www.ivanti.com/company/legal/privacy-policy

4.6. Availability

4.6.1 High-Availability Deployment

Ivanti designed the application to be multi-tenant with high levels of availability. Web application tiers are redundant in design with individually scalable application components, deployed across multiple fault-tolerant zones. Application and infrastructure monitoring are available to regulate flow of traffic automatically across these zones to maximize application performance and availability. Continuous monitoring detects anomalies, and self-healing processes reduce the need for human intervention and recovery.


High Availability Deployment and DR
High Availability Deployment
https://url
AWS
VPC
Leg 1
Lev 2
Leg 3
Zone1
Zone 2
Zone 3
HA Cluster 1
Customer Access
AWS
VPC
Leg 1
Leg 2
Leg 3
Zone 4
Zone 5
Zone 6
HA Cluster 2
High Availability Database Deployment
Local Site
Remote Site
Async
Sync
Listener
Windows Cluster
SQL Node 1 Primary Replica Automatic Failover
SQL Node 3 Primary Replica Automatic Failover
SQL Node 3 Primary Replica Automatic Failover


Blue-Green Deployment for Optimal Availability
Normal Operations
Step 1A: Disconnect one Leg
Step 1B: Upgrade the Disconnected Leg (Shown in Green)
Step 2: Move Service to Upgraded Leg (Green)
Step 3: Upgrade the Disconnected Leg
Step 4: Restore Normal Traffic
Load Balancer
Web Services
App Services
Database Services

4.6.2 Disaster Recovery

Ivanti uses always-on replication for near real-time replication of data to provide a low Recovery Point Objective (RPO) of 15 minutes, a Recovery Time Objective (RTO) of 4 hours, and to minimize data loss in the event of a naturally occurring or human-induced disaster. Ivanti uses hot backup sites for core services that Ivanti's 24X7 Network Operations Center (NOC) can switch to if deemed necessary. Customers choosing the advanced reporting option can get access to this read-only database for reporting purposes without impacting their transactional system.

4.6.3 24X7 Network Operations Center (NOC) and Security Operations Center (SOC)

Ivanti leverages an ISO27001-certified 24x7x365 network operations team, focused on Level 1 and Level 2 response with Level 3 and 4 staff on-call[2]. Ivanti monitors the NOC responses regularly for quality and adherence to SLA. Executive staff reviews NOC SLA reports to ensure optimal operations. The SOC actively monitors security incidents using a Security Incident and Event Management (SIEM) tool.

[2] Level 1 & Level 2: Incident response for known errors & responses with information gathering and troubleshooting and Level 3 & 4 support advanced troubleshooting, configuration and patch creation.

5. Conclusion

Cloud services are delivered by Ivanti's professional cloud-hosting organization with a level of data protection, availability, and performance standards that most mid-sized internal IT organizations would be challenged to meet. Ivanti's customers trust Ivanti to manage their most important systems as evidenced by significant growth, while Ivanti continues to invest aggressively to grow and improve cloud services.

For more information on Ivanti Cloud services and other products, please visit **www.ivanti.com.**

www.ivanti.com

☎ 1.800.982.2130

✉ sales@ivanti.com