REGIONE BASILICATA

PRESIDENZA GIUNTA REGIONALE

UFFICIO SPECIALE
PER L'AMMINISTRAZIONE DIGITALE

Via Vincenzo Verrastro, 6 – 85100 Potenza (PZ)
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

UFFICIO AMMINISTRAZIONE DIGITALE

Standard Tecnologici Regione Basilicata

CONTROLLO DEL DOCUMENTO:

Standard Tecnologici ver. 8.0

ultimo agg.: 29/05/2024

Sommario

1. Standard Tecnologici

Nel presente documento sono pubblicati gli standard tecnologici cui attenersi per l'attivazione, nel Data Center regionale, di servizi Cloud conformi alle procedure operative emanate da ACN(Agenzia per la Cybersicurezza Nazionale).

Nella tabella si sintetizzano le tecnologie e gli standard per le differenti tipologie di servizio Cloud IaaS, PaaS e SaaS di cui si richiede l'attivazione.

Il Data Center Unico Regionale ha implementato una soluzione di virtualizzazione avanzata basata su tecnologia VMware vSphere 8 Enterprise Plus.

Server		
Componente/Tecnologia	Soluzione Richiesta	Versione
Sistemi Operativi Server	• Microsoft Windows • Linux	Microsoft Windows 2016-2019-2022 Alma Linux 8.x - 9.x Rocky Linux 8.x - 9.x
Web Server	• Tomcat • Apache • IIS	ultima versione supportata
RDBMS	• MySQL (Open Source) • Postgres SQL (Open Source) • MS SQL Server • Oracle	ultima versione supportata previa verifica disponibilità previa verifica disponibilità-19g
Linguaggi	• Java • C# • .Net • Php • Html • Javascript	ultima versione supportata

Hosting		
Componente/Tecnologia	Soluzione Richiesta	Versione
Sistemi Operativi Server	• Microsoft Windows • Linux	Microsoft Windows 2016-2019-2022 Alma Linux 8.x - 9.x Rocky Linux 8.x - 9.x
Web Server	• Tomcat • Apache • IIS	ultima versione supportata

RDBMS	• MySQL (Open Source) • MS SQL Server • Oracle	MySql 8.0 previa verifica disponibilità previa verifica disponibilità-19g
Linguaggi	• Java • C# • .Net • Php • Html • Javascript	Php 8.0

2.Specifiche ed integrazione degli applicativi con il sistema Identity Management Regionale

La Regione Basilicata ha un sistema centralizzato di autenticazione degli utenti per l'accesso a tutte le applicazioni WEB presenti in Regione, sia quelle disponibili al cittadino che quelle utilizzate dai soli dipendenti regionali.

Il sistema centralizzato di autenticazione, d'ora in poi IDBroker, insieme a tutte le applicazioni WEB regionali forma un sistema di autenticazione federato; le applicazioni WEB riconosciute(federate) delegano il processo di autenticazione all'IDBroker e si fidano dell'identità dell'utente ottenuta.

La federazione delle applicazioni WEB regionali (d'ora in poi FRegBas) nonchè i messaggi scambiati con l'IDBroker sono basati sul framework SAML(Security Assertion Markup Language), in particolare SAML v2 profilo "Web Browser SSO" - "SAML V2.0 Technical Overview - Oasis par4.3".

La versione corrente dell'IDBroker (v1.0.10) è retrocompatibile con la precedente versione di IdP Regionale denominato IMS. A breve verrà rilasciata una nuova versione dell'IDBroker (v2.0.0) con dei requisiti di integrazione più restrittivi. Si riportano, di seguito, le specifiche compatibili con la versione corrente e consigliate per nuove applicazioni.

Metadati

I metadati dell'IdP Regionale sono disponibili all'url: https://spid.regione.basilicata.it/metadata/idp/idp-metadata.xml

Anche i gestori delle applicazioni WEB registrate sull'IDBroker dovranno rendere disponibili i propri metadati SAML tramite una URL https.

I metadati delle applicazioni WEB registrate sull'IDBroker devono, inoltre, rispettare le seguenti condizioni:

- nell'elemento EntityDescriptor deve essere presente l'attributo "entityID" (1 occorrenza);
- deve essere presente un solo elemento SPSSODescriptor con l'attributo "protocolSupportEnumeration" valorizzato a "urn:oasis:names:tc:SAML:2.0:protocol";
- deve essere presente un elemento "AssertionConsumerService" con l'attributo "Binding" valorizzato a "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" e con l'attributo "Location"non vuoto;

Attributi

Gli attributi certificati dall'IDBroker nelle asserzioni SAML compatibili anche con la prossima versione di IDBroker (v2.0.0) sono i seguenti: identitySystem, validate, spidCode, name, familyName, fiscalNumber, dateOfBirth.

L'attributo urn:oid:identitySystem attesta la modalità di autenticazione effettuata dall'utente e può assumere i seguenti valori: SPID, CIE, EIDAS, LEGACY_REGBAS.

L'attributo urn:oid:validate attesta il livello di autenticazione come da specifiche SPID e può assumere i valori:

https://www.spid.gov.it/SpidL1,

https://www.spid.gov.it/SpidL2,

https://www.spid.gov.it/SpidL3

Per gli altri attributi fare riferimento alle specifiche SPID.

Come ottenere la federazione

I gestori degli applicativi Regionali che intendono federarsi in FRegBas dovranno fornire le seguenti informazioni:

1) url dei metadati dell'applicativo Regionale da integrare;
2) Livello di sicurezza minimo richiesto dall'applicativo Regionale (SPID Livello 1, 2 o 3)

Per ulteriori chiarimenti contattare l'ufficio Amministrazione Digitale.

3. Misure per garantire la sicurezza delle applicazioni informatiche installate nel data center unico regionale

L'Ufficio Speciale per l'Amministrazione Digitale della Regione Basilicata, al fine di garantire la sicurezza delle applicazioni informatiche di proprietà regionale installate nel Data Center regionale, adotta i seguenti standard tecnologici mediante l'uso di sistemi di Software intelligence Analisys:

- Standard ISO/IEC 5055:2021 per l'analisi della qualità strutturale, delle performance e
  dei rischi degli applicativi e delle forniture software;
- Standard ISO 19515:2019 per calcolare la dimensione della baseline applicativa effettiva mediante la tecnica degli AFP-Automated Function Point e misurare le MEV sulle applicazioni;
- Standard ISO 5320 per effettuare la Software Composition Analysis;
- Standard OWASP e MITRE per le verifiche di vulnerabilità e fattori critici di sicurezza;
- Standard ISO/IEC 19506:2012 per ricostruire l'architettura software degli applicativi e le loro interazioni, preservando così la conoscenza strategica dell'amministrazione sui propri asset digitali;

Attraverso l'utilizzo della piattaforma CAST AIP (Cast Engineering Dashboard e Cast Health Dashboard), vengono analizzati in profondità tutti gli aspetti relativi alla sicurezza intrinseca degli applicativi in ambito, alla qualità strutturale e alla dimensione funzionale del software. Vengono rilevate le debolezze strutturali di sicurezza contenute negli applicativi, con un'analisi di tipo SAST (Static Application Security Testing), nonché le vulnerabilità, note o latenti, contenute nelle librerie Open Source utilizzate all'interno delle applicazioni.

Tali misurazioni sono effettuate automaticamente su tutti i rilasci del software dei fornitori prima della messa in produzione in modo da poter minimizzare i rischi operativi (resilienza, efficienza, sicurezza e manutenibilità) e quantificare l'effettivo volume delle forniture stesse.

Mediante l'uso di una serie di strumenti integrati utilizzati dal Centro di Competenza di Software Engineering della Regione Basilicata, sono realizzati i quattro pilastri di base della disciplina di misurazione:

- Misurazione del rischi software;
- Misurazione della dimensione funzionale;
- Mitigazione dei rischi e remediation plan;
- Modernizzazione del software.

Per i software in licenza d'uso, l'utente dovrà fornire analoghe garanzie e certificazioni.

Indicatori CAST:

NOME APPLICAZIONE	Il nome dell'applicazione identifica il perimetro del software che è stato analizzato e deve coincidere con quello indicato nel Catalogo Software di Regione Basilicata.
DIMENSIONE TECNICA (TECHNICAL SIZE)	Nel Technical Size sono riportate le linee di codice (LOC) dell'applicazione depurate da codice generato automaticamente e codice relativo a librerie o componenti di terze parti.
ROBUSTEZZA (ROBUSTNESS)	La Robustness dell'applicazione è un indice della sua capacità di resistere a cambiamenti senza introdurre bugs o malfunzionamenti. Scala di valori: da 1.0 a 4.0. Soglia di rischio: 3.0
EFFICIENZA (EFFICIENCY)	L'Efficiency è un indice di performance dell'applicazione in termini di velocità e di consumo di risorse (memoria,rete, connesisoni,cpu). Più il codice sorgente è efficiente nella gestione dei cicli e nell'allocazione/disallocazione di risorse, più l'applicazione fornirà le risposte attese in tempi brevi e sarà possibile farla funzionare anche su un hardware di dimensioni ridotte, senza il rischio di blocchi o malfunzionamenti. Scala di valori: da 1.0 a 4.0. Soglia di rischio: 3.0
SICUREZZA (SECURITY)	La Security dell'applicazione è data dalla quantità di violazioni di pratiche di sicurezza volte a impedire possibili intrusioni da parte di utenti malintenzionati o per garantire il corretto funzionamento dell'applicazione, prevenendo ogni possibile causa di corruzione dei dati o di comportamenti inattesi del software. Scala di valori: da 1.0 a 4.0. Soglia di rischio: 3.0
MODIFICABILITA' (CHANGEABILITY)	La Changeability indica quanto facilmente l'applicazione può essere modificata tenendo sotto controllo l'effort e di conseguenza i costi necessari per il suo mantenimento. Scala di valori: da 1.0 a 4.0. Soglia di rischio: 3.0
(TRASFERIBILITA') TRANSFERABILITY	La Transferability indica quanto facilmente il codice sorgente dell'applicazione può essere compreso da una nuova risorsa che viene inserita nel team di sviluppo, oppure il costo del trasferimento del suo mantenimento da un team ad un altro. Scala di valori: da 1.0 a 4.0. Soglia di rischio: 3.0
FUNCTIONAL& ENHANCEMENT SIZE (AEP)	Dimensione Funzionale relativa soltanto a tutte le componenti aggiunte/modificate/cancellate nell'applicazione nel periodo compreso tra l'analisi precedente e l'attuale (snapshot).

OMG-COMPLIANT AUTOMATED FPS (AFP)	Dimensione Funzionale complessiva dell'applicazione calcolata secondo lo standard OMG-ISO-5055. Il conteggio è composto da due componenti: - DATA FUNCTIONS (conteggio relativo ai dati movimentati dall'applicazione) - TRANSACTIONAL FUNCTIONS (conteggio relativo alle funzionalità esposte agli utenti)
VIOLAZIONI CRITICHE (CRITICAL VIOLATIONS)	Le Violazioni Critiche sono un sottoinsieme delle violazioni individuate da CAST MRI per tutte le regole del modello di qualità. Le Violazioni Critiche sono le violazioni delle regole che sono marcate come critiche all'interno del modello: tali regole sono quelle che hanno un impatto maggiore sugli indici di qualità e quindi comportano un rischio maggiore. **NB. L'aggiunta di violazioni critiche non sarà permessa per gli sviluppi da portare in produzione.**

Fornitura delle componenti software degli applicativi

Per poter essere analizzato e misurato in modo corretto, il codice sorgente compreso nel perimetro delle applicazioni deve essere caricato sul repository di Regione Basilicata rispettando alcuni criteri:

- Deve essere caricato il codice sorgente completo delle applicazioni, rispettando la struttura di cartelle del codice presente sull'IDE di sviluppo;
- La struttura dei sorgenti per la stessa applicazione deve essere riproducibile per consentire la coerenza durante l'analisi successiva;
- Devono essere escluse le cartelle ed il codice contenente unit-test o altri tipi di test, devono essere esclusi codici di esempio o altro codice che non implementa le funzionalità effettivamente esposte dall'applicazione;
- Lo stesso codice sorgente va caricato una volta sola: non devono esserci doppioni contenenti gli stessi sotto progetti in diversi punti dell'alberatura.
- Devono essere inclusi i files di progetto che vengono utilizzati per creare la build (versione compilata per il deploy in produzione). (p.e. POM.XML di Maven);
- Devono essere incluse tutte le librerie di terze parti utilizzate, sia nel caso di librerie open source con codice in chiaro (es. librerie Javascript: file .js o .json) che compilate (es. files .dll o .jar)
- Nel caso in cui l'applicazione mantenga un database considerato parte del perimetro applicativo, vanno incluse le DDL (Data Definition Language) estratte dagli schemi database utilizzati. Le DDL devono essere allineate con la versione degli altri sorgenti forniti.
- Nel caso di applicazioni composte da più sotto progetti, ogni sotto progetto va inserito in una apposita sottocartella all'interno del root dell'applicazione, in più sarà presente una sottocartella specifica per le DDL

Per una verifica esaustiva dei requisiti per il caricamento dei sorgenti per ciascuna tecnologia coperta dagli analizzatori di CAST, si rimanda alla documentazione online:

https://doc.castsoftware.com/display/FBP/Source+Code+Delivery+Instructions
https://doc.castsoftware.com/display/TECHNOS
Il caricamento dei sorgenti delle applicazioni e l'ulteriore documentazione tecnica dovranno avvenire sul repository GitLab di Regione Basilicata.